# bitdefender 9

Standard

## Guia de usuário

- Antivírus
- Anti-spam
- Firewall

Copyright © 2006 SOFTWIN

# BitDefender 9 Standard
*Guia de usuário*

**SOFTWIN**

Publicado 2006.04.19
Build 9.5

Copyright © 2006 SOFTWIN

## Nota Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida em qualquer forma e meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou qualquer armazenamento e recuperação de informações, sem permissão escrita da SOFTWIN, exceto para a inclusão de breve citações em revisões. O conteúdo não pode ser modificado em qualquer modo.

**Aviso.** Este produto e sua documentação são protegidos por direitos autorais. A informação neste documento é providenciada na sua própria essência, sem garantias. Apesar de todas as precauções terem sido tomadas na preparação deste documento, os autores não têm responsabilidade sobre qualquer pessoa ou entidade em respeito à perda ou dano causado direta ou indiretamente pela informação contida neste documento..

Este livro contem referências a páginas web terceiras que não estão sob o controle da SOFTWIN, e a SOFTWIN não é responsável pelo conteúdo de nenhum site de referência. Se você acessar alguma página web de terceiros mencionadas neste guia, será por sua conta e risco. A SOFTWIN providencia estas referências por pura conveniência, e a inclusão da referência não implica que a SOFTWIN assimila ou aceita qualquer responsabilidade pelo conteúdo dos sites terceiros.

**Marcas Registradas.** Nomes de marcas registradas podem aparecer neste livro. Todas as marcas registradas ou não registradas neste documento são de propriedade única de seus respectivos donos.

bitdefender
secure your every bit

# Índice

**Licença e garantia** ..... ix

**Prefácio** ..... xiii

1. Convenções usadas neste livro ..... xiii
   1.1. Convenções tipográficas ..... xiii
   1.2. Avisos ..... xiv
2. A estrutura do livro ..... xiv
3. Convite a Comentários ..... xv

## Instalação do Produto ..... 17

**1. Instalação do BitDefender 9 Standard** ..... 19
   1.1. Requisitos Mínimos ..... 19
   1.2. Passos de instalação ..... 19
   1.3. Atualização de versão ..... 22
   1.4. Remoção, reparo ou modificação das funções do BitDefender ..... 22

## Descrição e Funções ..... 25

**2. Sumário** ..... 27
   2.1. Por que BitDefender? ..... 27
   2.2. Data Security Division ..... 28
   2.3. SOFTWIN ..... 29

**3. BitDefender 9 Standard** ..... 31
   3.1. Antivírus ..... 31
   3.2. Outros Recursos ..... 32

**4. Módulos do BitDefender** ..... 33
   4.1. Módulo Geral ..... 33
   4.2. Módulo Antivírus ..... 33
   4.3. Módulo Atualização ..... 33

## Console de Gerenciamento ..... 35

**5. Visão Geral** ..... 37
   5.1. Barra de tarefas ..... 38
   5.2. Barra de atividade de verificação ..... 39

**6. Módulo Geral** ..... 41
   6.1. Informação geral ..... 41

6.1.1. Virus Shield . . . . . 42
6.1.2. Atualização Automática . . . . . 43
6.2. Registro do Produto . . . . . 43
6.3. Configurações da console de gerenciamento . . . . . 44
6.4. Eventos . . . . . 47
6.5. Sobre . . . . . 49

**7. Módulo do Antivírus . . . . . 51**
7.1. Verificação no-acesso . . . . . 51
7.1.1. Controle de Registro . . . . . 52
7.1.2. As opções mais importantes . . . . . 54
7.1.3. Outras opções . . . . . 55
7.2. Verificação solicitada . . . . . 57
7.2.1. Verificação imediata . . . . . 59
7.2.2. Verificação contextual . . . . . 67
7.2.3. Verificação Arraste & Solte . . . . . 67
7.2.4. Verificação agendada . . . . . 69
7.3. Quarentena . . . . . 80
7.4. Relatório . . . . . 83

**8. Módulo de Atualização . . . . . 87**
8.1. Atualização automática . . . . . 87
8.2. Atualização Manual . . . . . 89
8.2.1. Atualização manual com `weekly.exe` . . . . . 89
8.2.2. Atualização manual com `arquivos zip` . . . . . 89
8.3. Configurações . . . . . 91
8.3.1. Configurações do local para atualização . . . . . 92
8.3.2. Opções para atualização automática . . . . . 93
8.3.3. Configurações de atualização manual . . . . . 94
8.3.4. Opções avançadas . . . . . 94

Melhores práticas . . . . . 95

**9. Melhores práticas . . . . . 97**
9.1. Antivírus . . . . . 97

CD de Resgate BitDefender . . . . . 99

**10. Resumo . . . . . 101**
10.1. O que é KNOPPIX? . . . . . 101
10.2. Requisitos Mínimos . . . . . 101
10.3. Software incluído . . . . . 102
10.4. Soluções BitDefender para Linux . . . . . 103
10.4.1. BitDefender SMTP Proxy . . . . . 103
10.4.2. BitDefender Remote Admin . . . . . 103
10.4.3. BitDefender Linux Edition . . . . . 104

**11. Guia LinuxDefender . . . . . 105**
11.1. Iniciar e parar . . . . . 105
11.1.1. Iniciar LinuxDefender . . . . . 105
11.1.2. Parar LinuxDefender . . . . . 107
11.2. Configure a conexão de Internet . . . . . 108
11.3. Atualização BitDefender . . . . . 108
11.4. Verificação de Vírus . . . . . 109
11.4.1. Como acessar os dados do Windows? . . . . . 109
11.4.2. Como executo uma verificação antivírus? . . . . . 110
11.5. Construindo um filtro instantâneo de e-mail . . . . . 110
11.5.1. Pré-requisitos . . . . . 110
11.5.2. O Filtro de e-mail . . . . . 111
11.6. Exexutar auditoria de segurança de rede . . . . . 112
11.6.1. Verificar rootkits . . . . . 112
11.6.2. Nessus – O Verificador de Rede . . . . . 112
11.7. Verifique a RAM do seu sistema . . . . . 113

Ajuda . . . . . 115

**12. Suporte . . . . . 117**
12.1. Departamento de suporte . . . . . 117
12.2. Ajuda on-line . . . . . 117
12.2.1. BitDefender Knowledge Base . . . . . 117
12.3. Informação sobre contato . . . . . 118
12.3.1. Endereços Web . . . . . 118
12.3.2. Endereço . . . . . 118

**13. Perguntas Mais Freqüentes . . . . . 121**

**Vocabulário . . . . . 123**

# Licença e garantia

Este Contrato de Licença representa um acordo legal entre Você (como pessoa física ou jurídica) e a SOFTWIN S.R.L.. Este produto de software pertence a SOFTWIN S.R.L., e inclui o software e também o meio físico adjunto, os impressos, e também a documentação eletrônica do BitDefender. Tudo isso está protegido pela legislação interna e internacional referente ao copyright e propriedade intelectual. A instalação, a cópia ou outra maneira de utilização do produto BitDefender, significa o aceite dos termos deste contrato. Se não estiver de acordo com certa(s) cláusula(s), não instale e não utilize BitDefender. Se não estiver satisfeito com o produto, você dispõe de um prazo de 30 dias para devolvê-lo ao estabelecimento onde o adquiriu e onde lhe será devolvido o valor pago. Será necessário apresentar o comprovante de compra.

BitDefender está protegido pelas leis de direitos do autor (copyright), as leis da propriedade intelectual e outros tratados internacionais que são desta aplicação. O produto de software BitDefender é um produto com licença. A licença acompanha o produto e não é vendida separadamente.

OUTORGAR A LICENÇA: SOFTWIN oferece as seguintes condições para a licença do BitDefender:

APLICAÇÃO SOFTWARE. O comprador pode instalar e usar o produto BitDefender, ou qualquer versão anterior que funcione com o mesmo sistema operacional e somente em um computador

UTILIZAÇÃO NA REDE. O comprador pode instalar BitDefender em um servidor, ou em outros equipamentos da rede, mas deve comprar uma licença para cada equipamento onde está instalado BitDefender. Uma mesma licença BitDefender não se permite utilizar em computadores distintos

O PACOTE DE LICENÇAS. Se houver recebido este contrato de licença para múltiplas licenças, o comprador pode realizar um número adicional de cópias do produto BitDefender, segundo o número de licenças adquiridas. Pode-se utilizar cada cópia da maneira especificada anteriormente.

TERMOS DA LICENÇA. A presente licença estará garantida e entrará em vigor a partir da data da compra, cópia ou utilização. Será válida somente para o equipamento onde se instala o programa.

ATUALIZAÇÕES DO PRODUTO (UPGRADE). Para se ter o serviço de “upgrade” do produto BitDefender, deve ser um usuário com licença. BitDefender inclui como

"upgrade" a versão atual que substitua e/ou substituirá o produto básico com licença. O comprador pode utilizar o produto atualizado nas condições estipuladas nos termos do presente contrato. Se BitDefender foi atualizado em um equipamento estará terminantemente proibido utilizá-lo em outros equipamentos

COPYRIGHT. Todos os direitos, o título e todos os benefícios como os direitos de cópia acerca de BitDefender são propriedade de SOFTWIN S.R.L.. O produto BitDefender incluindo todas as fotos, animações, imagens de vídeo, áudio, texto, "applets" e os materiais adjuntos, impressos ou outras cópias do mesmo são propriedade de SOFTWIN S.R.L. e estão protegidas pelas leis e tratados internacionais de direitos do autor e propriedade intelectual. Nem a documentação, nem os programas incluídos neste pacote podem ser copiados, reproduzidos, ou traduzidos em qualquer mídia ou meio eletrônico legível sem a permissão prévia por escrito da SOFTWIN S.R.L.. O comprador tem a obrigação de incluir todos os documentos originais de Copyright para todas as cópias criadas independentemente da mídia de gravação ou do BitDefender adquirido. Está proibido entregar licenças e também alugar, vender, ou realizar "leasing" para o produto BitDefender.

LIMITES DA GARANTIA. SOFTWIN S.R.L. garante o funcionamento do programa BitDefender, de acordo com o especificado no manual de ajuda pelas telas incluídas neste produto durante trinta dias à partir da data de recebimento. Se o CD incluído neste pacote BitDefender, apresentar defeitos que impeçam o bom funcionamento do programa neste prazo, a empresa SOFTWIN S.R.L. garante ao usuário a reparação e a substituição do produto, sempre que estiver acompanhado pelo certificado de licença e o comprovante de compra. O presente contrato de licença, SOFTWIN S.R.L. não requer uma outra garantia especificada ou um original para BitDefender. Esta licença é exclusiva e substitui qualquer outra garantia, especificada ou original, incluindo a garantia original de comercialização ou de uso individual. Esta garantia oferece todos os direitos legais específicos. ESTA GARANTIA NÃO COBRE O MATERIAL PERDIDO, ROUBADO OU DANIFICADO DE FORMA ACIDENTAL, UTILIZADO INDEVIDAMENTE OU MODIFICADO SEM AUTORIZAÇÃO.

TERMOS LEGAIS. Os usuários que analisam, testam ou avaliam BitDefender serão responsáveis pelos danos que podem ocorrer pelo uso incorreto do produto. Em nenhum caso, SOFTWIN S.R.L. se responsabiliza por qualquer tipo de dano, incluindo, os danos diretos ou indiretos que derivem da utilização do produto BitDefender embora a existência da possibilidade de ocorrer tais danos tenha sido advertida pela SOFTWIN S.R.L.. As condições estipuladas nesta seção se aplicarão se aceitas, utilizadas, avaliadas ou provadas por BitDefender.

NOTA IMPORTANTE PARA OS USUÁRIOS. ESTE SOFTWARE PODE CONTER ERROS, E NÃO É INDICADA SUA UTILIZAÇÃO EM NENHUM MEIO QUE REQUERA UM ALTO GRAU DE RISCO E QUE NECESSITE ALTA ESTABILIDADE. ESTE

PRODUTO DE SOFTWARE NÃO ESTÁ DESTINADO A SETORES DAS ÁREAS DE AVIAÇÃO, CENTRAIS NUCLEARES, SISTEMAS DE TELECOMUNICAÇÕES, ARMAS, OU SISTEMAS RELACIONADOS COM A SEGURANÇA DIRETA OU INDIRETA DA VIDA. TÃO POUCO ESTÁ INDICADO PARA APLICAÇÕES OU INSTALAÇÕES ONDE UM ERRO DE FUNCIONAMENTO PODERIA PROVOCAR A MORTE, DANOS FÍSICOS OU DANOS CONTRA A PROPRIEDADE.

GOVERNMENT RESTRICTED RIGHTS/RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable. Contact SOFTWIN, at 5, F-ca de Glucoza str., 72322-Sect.2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763.

GERAL. Este contrato está sujeito às leis brasileiras e internacionais. Pode ser modificado adicionando-se um anexo em duas vias, ou um documento firmado e selado por ambas as partes, você e a SOFTWIN S.R.L.. Este contrato estará em português e não será traduzido ou interpretado em nenhum outro idioma.Os preços, custos e tarifas para BitDefender podem ser objeto de algumas modificações sem aviso prévio. Na eventualidade de uma invalidez de qualquer cláusula do presente Contrato de Licença, a invalidez não afetará as outras partes componentes do presente contrato. BitDefender e BitDefender logos são marcas registradas de SOFTWIN S.R.L.. Microsoft Windows, Excel, Word, o logo do Windows, Windows NT, Windows 2000 são marcas registradas da Microsoft Corporation. Outras marcas registradas pertencem a seus proprietários.

# Prefácio

Este é direcionado para todos os usuários que escolheram o **BitDefender 9 Standard** como a solução de segurança em seus computadores pessoais. A informação apresentada neste livro é aplicada não somente para usuários avançados de computação, mas também para qualquer pessoa que esteja apta a trabalhar com o sistema Windows.

Este livro irá descrever para você o **BitDefender 9 Standard**, a empresa e o time que o construiu, irá guiá-lo através do processo de instalação e o ensinará como configurá-lo. Você irá descobrir como usar o **BitDefender 9 Standard**, como atualizar, testar e customizá-lo. Você aprenderá como aproveitar melhor o BitDefender.

Desejamos a você uma agradável e útil leitura.

## 1. Convenções usadas neste livro

### 1.1. Convenções tipográficas

Vários estilos de texto são usados para implementar a leitura. O aspecto e significado dos mesmos estão representados na tabela abaixo.

| Aparência | Descrição |
|---|---|
| `exemplo de sintaxe` | Exemplos de sintaxe são impressos em caracteres do tipo `monospaced`. |
| http://www.bitdefender.com | As referências URL apontam para algum local externo, em servidores http ou ftp. |
| <support@bitdefender.com> | Mensagens de e-mail são inseridas no texto para informação sobre contato. |
| “Prefácio” (p. xiii) | Este é uma referência interna, a algum lugar dentro do documento. |
| `arquivo` | Arquivos e pastas são impressos em caracteres do tipo `monospaced`. |

| Aparência | Descrição |
| --- | --- |
| **opção** | Todas as opções do produtos são impressas em **negrito**. |
| `exemplo de lista de código` | Listas de código são impressos em caracteres do tipo `monospaced`. |

## 1.2. Avisos

Os avisos estão em notas de texto, graficamente marcados, chamando a sua atenção para informação adicional relacionado ao parágrafo atual.

### Nota

A nota é apenas uma breve observação. As notas providenciam informação valiosa, assim como uma função específica ou uma referência sobre um tópico relacionado.

### Importante

Este requer sua atenção e não é recomendado deixar escapar. Normalmente providencia informação não crítica mas significante.

### Atenção

Esta é uma informação crítica e deve ser tratada com cautela. Nada ruim acontecerá se você seguir as indicações. Você deve ler e entender tal informação, ela descreve algo de extreme risco.

# 2. A estrutura do livro

O livro consiste em seis partes, contendo os tópicos mais importantes: Instalação do Produto, Descrição e Funções, Console de Gerenciamento, Melhores Práticas, CD de Resgate BitDefender e Ajuda. Além disso, um glossário está disponível para esclarecer alguns termos técnicos.

**Instalação do Produto.** Instruções passo a passo para instalar o BitDefender em uma estação de trabalho. Este é um tutorial compreensivo de como instalar o **BitDefender 9 Standard**. Começando com os pré-requisitos para uma instalação de sucesso, você será guiado através de todo o processo de instalação. Finalmente, o procedimento de remoção é descrito caso você precisa desinstalar o BitDefender.

**Descrição e Funções.** Um curta introdução ao BitDefender. Explica quem é BitDefender is, quem são SOFTWIN e Data Security Division. O **BitDefender 9 Standard**, suas funções e os módulos do produto são apresentadas a você.

**Console de Gerenciamento.** Descrição da administração básica e manutenção do BitDefender. Os capítulos explicam em detalhes todas as opções do **BitDefender 9 Standard**, como registrar o produto, como verificar seu computador e como executar as atualizações.

**Melhores Práticas.** Siga os passos descritos nesta seção para garantir um computador seguro.

**CD de resgate BitDefender.** Descrição do CD de resgate BitDefender. Ajuda a compreender e utilizar as ferramentas oferecidas por este Cd de boot.

**Ajuda.** Onde procurear e onde perguntar por ajuda caso algo aconteça for a do esperado. Uma seção de perguntas e respostas também está disponível.

**Glossário.** O Glossário tenta explicar alguns termos técnicos e incomuns que você pode encontrar nas páginas deste documento.

## 3. Convite a Comentários

Nós convidamos você a nos ajudar a melhorar o livro. Nós testamos e verificamos todas as informações na nossa habilidade. Por favor nos escreva sobre qualquer falha que você encontrar neste livro ou como você pensa que ele possa ser melhorado, para nos ajudar a providenciar a melhor documentação possível.

Mande-nos um e-mail para <documentation@bitdefender.com>.

# Instalação do Produto

# 1. Instalação do BitDefender 9 Standard

A seção **Instalação do BitDefender 9 Standard** deste guia de usuário contem os seguintes tópicos:

- Requisitos Mínimos
- Passos da instalação
- Atualização de versão
- Remoção, reparo ou modificação das funções do BitDefender

## 1.1. Requisitos Mínimos

Para garantir um funcionamento apropriado do produto, antes da instalação, verifique que os requisitos mínimos do seu sistema sejam:

- **Mínimo de Processador** - Pentium MMX 200 MHz
- **Mínimo de espaço em disco rígido** - 40MB
- **Mínimo de Memória RAM** - 64MB (128MB Recomendada)
- **Sistema Operacional** - Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 5.5 (+)

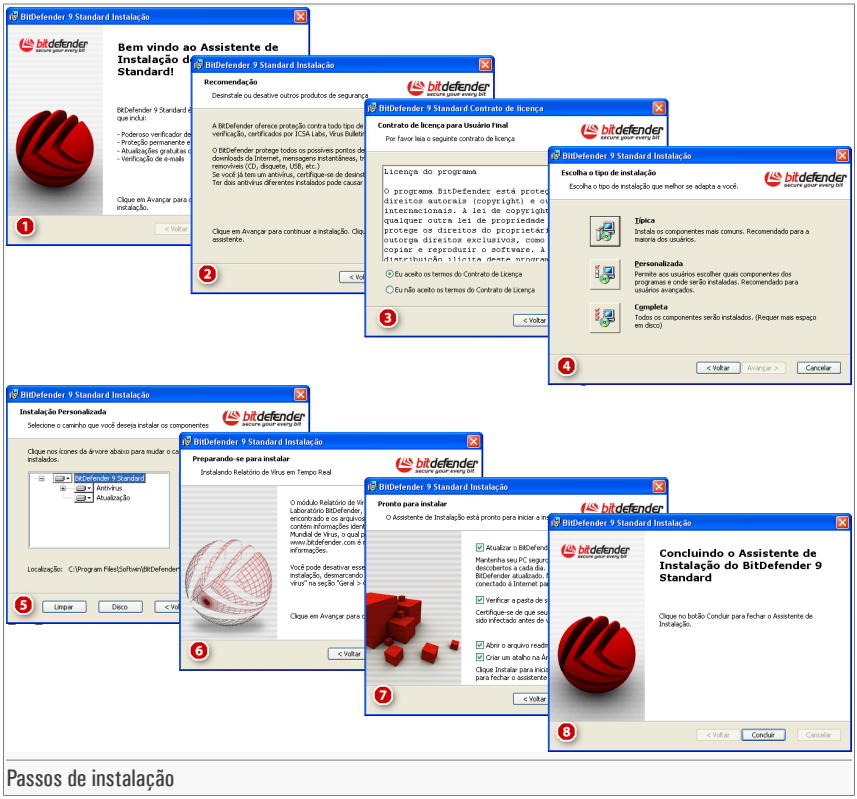
Atenção

O **BitDefender 9 Standard** não pode ser instalado no Windows NT 4.0 Server, Windows 2000 Server ou Windows 2003 Server. Para estas plataformas recomendamos os produtos corporativos para servidores de arquivo, gateways e servidores de e-mail.

## 1.2. Passos de instalação

Localize o arquivo de configuração e clique duplamente sobre ele. Um assistente será carregado e irá guiá-lo através do processo de configuração:

Passos de instalação:


BitDefender 9 Standard Instalação
Bem vindo ao Assistente de Instalação d
Standard!
Recomendação
Desinstale ou desative outros produtos de segurança
BitDefender 9 Standard Contrato de licença
Contrato de licença para Usuário Final
Por favor leia o seguinte contrato de licença
Licença do programa
Eu aceito os termos do Contrato de Licença
Eu não aceito os termos do Contrato de Licença
Escolha o tipo de instalação
Escolha o tipo de instalação que melhor se adapta a você.
Típica
Instala os componentes mais comuns. Recomendado para a maioria dos usuários.
Personalizada
Permite aos usuários escolher quais componentes dos programas e onde serão instaladas. Recomendado para usuários avançados.
Completa
Todos os componentes serão instalados. (Requer mais espaço em disco)
< Voltar
Avançar >
Cancelar
Instalação Personalizada
Selecione o caminho que você deseja instalar os componentes
Antivirus
Atualização
Limpar
Disco
Preparando-se para instalar
Instalando Relatório de Vírus em Tempo Real
Pronto para instalar
O Assistente de Instalação está pronto para iniciar a instalação.
Concluindo o Assistente de Instalação do BitDefender 9 Standard
Clique no botão Concluir para fechar o Assistente de Instalação.
Concluir

Passos de instalação

1. Clique em **Avançar** para continuar ou clique **Cancelar** se você quiser sair da instalação.

2. Clique em **Avançar** para continuar ou clique **Anterior** para retornar ao primeiro passo.

3. Leia o Acordo de Licenciamento, selecione **Eu aceito os termos no Acordo de Licenciamento** e clique **Avançar**. Se você não concordar com estes termos, clique em **Cancelar**. O processo de instalação será abandonado e você sairá da configuração.

4. Você pode escolher que tipo de instalação você deseja: típica, customizada ou completa.

- **Típica** - O programa será instalado com as mais comuns opções. Esta opção é a recomendada para a maioria dos usuários.
- **Customizada** - Você pode escolher os componentes que deseja instalar. Recomendada para usuários avançados apenas.
- **Completa** - Para instalação completa do produto. Todos os módulos BitDefender serão instalados.

  Se você selecionar **Típica** ou **Completa** você escapará o passo 5.

5. Se você selecionou **Customizada**, uma nova janela aparecerá contendo todos os componentes BitDefender listados para que você selecione os que deseja instalar.

   Se você clicar em qualquer componente, uma breve descrição (incluindo o mínimo de espaço requerido em disco rígido) aparecerá ao lado direito. Se você clicar em qualquer ícone de componente uma janela aparecerá onde você pode instalar ou não o módulo selecionado.

   Você pode selecionar a pasta onde você pode instalar o produto. A pasta padrão é `C:\Program Files\Softwin\BitDefender 9`.

   Se você deseja selecionar outra pasta, clique **Procurar** e na janela que aparecerá, selecione a pasta que você deseja que o BitDefender seja instalado. Clique em **Avançar**.

6. Clique em **Avançar**.

7. Você tem quarto opções selecionadas por padrão:

   - **Atualizar o BitDefender** - para atualizar o BitDefender no final da instalação. Seu sistema de estar conectado a Internet para atualizar.
   - **Verificar a pasta de sistema do Windows** - para rastrear a pasta de sistema do windows ao fim da instalação.
   - **Abra o arquivo readme** - para abrir o arquivo leiame no final da instalação.
   - **Criar um atalho no desktop** - para colocar um atalho do BitDefender no seu desktop no final da instalação.

   Clique em **Instalar** para começar a instalação do produto.

8. Clique em **Finalizar** para completar a instalação do produto. Se você aceitou a configuração padrão para o local de instalação, uma nova pasta chamada `Softwin` será criada em `Arquivos de Programas` e conterá a pasta `BitDefender 9`.

**Nota**
Você pode ter que reiniciar seu sistema para que o assistente complete o processo de instalação.

## 1.3. Atualização de versão

O procedimento de atualização de versão pode ser feito das seguintes maneiras:

- Instalar sem remover a versão anterior - apenas da v8 para a v9

  Clique duas vezes no arquivo de configuração e siga o assistente como descrito no seção "*Passos de instalação*" (p. 19).

**Importante**
Durante o processo de instalação uma mensagem de erro causada pelo `serviço Filespy` aparecerá. Clique em **OK** para continuar a instalação.

- Desinstale a versão anterior e instale a nova versão - para todas as versões do BitDefender

  Primeiro você terá que remover a versão anterior, reiniciar o computador e instalar a nova versão como descrito na seção "*Passos de instalação*" (p. 19).

**Importante**
Se você estiver atualizando a versão 8 para a 9 nós recomendamos que você salve as Configurações BitDefender . Depois do processo de atualização ser concluído, você poderá carregar estas configurações novemente.

## 1.4. Remoção, reparo ou modificação das funções do BitDefender

Se você deseja modificar, reparar ou remover o **BitDefender 9 Standard**, siga o caminho no Windows: **Iniciar** -> **Programas** -> **BitDefender 9** -> **Modificar, Reparar ou Desinstalar**.

Você terá que confirmar a opção clicando em **Próximo**. Uma nova janela aparecerá e você pode selecionar:

- **Modificar** - para selecionar componentes para instalar ou remover;
- **Reparar** - para reinstalar todos os componentes do programa;

Importante

Antes de reparar o produto recomendamos que você salve as Configurações do BitDefender. Depois do processo de reparação terminar você pode carregá-los novamente.

- **Remover** - para remover todos os componentes instalados.

Para continuar a configuração, selecione uma das três opções listadas acima. Nós recomendamos que você escolha **Remover** para uma melhor reinstalação. Depois do processo acabar, recomendamos que você apague a pasta `Softwin` do `Arquivo de Programas`.

# Descrição e Funções

# 2. Sumário

O BitDefender providencia soluções de segurança para satisfazer os requerimentos de segurança do ambiente computacional atual, entregando gerenciamento a ameaças a mais de 43 milhões de usuários domésticos e corporativos em mais de 100 países.

Desenvolvido para providenciar uma proteção completa para redes e sistemas corporativos, a solução BitDefender compreende, além de proteção antivírus, anti-spam, firewall pessoal e soluções de gerenciamento de segurança. O BitDefender também se especializa em providenciar assistência com desenvolvimento e estabelecimento de políticas de segurança para usuários corporativos.

O BitDefender Professional foi o terceiro produto de linha a receber a certificação ICSA para Windows XP e o primeiro a ser premiado por inovação pelo European Commission and Academies. O BitDefender Antivirus é certificado por todos os principais revisores na área de antivírus - ICSA Labs, CheckMark, CheckVir, TÜV e Virus Bulletin.

O BitDefender tem sua matriz localizada em Bucareste, Romênia e possui escritórios em Tettnang, Alemanha, Barcelona, Espanha e Flórida, EUA. Página da web: http://www.bitdefender.com

## 2.1. Por que BitDefender?

**Comprovado. Maior produtor de reatividade de antivírus.** A rápida reatividade do BitDefender em caso de epidemia de vírus foi confirmado nas últimas epidemias de CodeRed, Nimda and Sircam, assim como Badtrans.B e outras pragas de rápida infecção. O BitDefender foi o primeiro a providenciar antídotos contra estes códigos e a providenciar vacinas gratuitas na Internet para todas as pessoas afetadas. Agora com a expansão contínua do vírus Klez – em várias versões, uma proteção antivírus se tornou crítica para qualquer sistema computacional.

**Inovação. Premiado por inovação pelo European Commission e EuroCase.** O BitDefender foi proclamado vencedor do European IST-Prize, premiado pelo European Commission e seus representantes de 18 academias na Europa. Agora em seu oitavo ano, o European IST Prize é um reconhecimento de produtos inovadores que representam o melhor da tecnologia de informação da Europa.

**Compreensivo. Protege todos os pontos de sua rede, providenciando segurança completa.** As soluções de segurança BitDefender para ambientes corporativos satisfazem os requerimentos de proteção do ambiente atual de negócios, habilitando gerenciamento de todas as ameaças complexas que se tornam um perigo para a rede, desde uma rede local a WANs de multi-plataforma.

**Sua Melhor Proteção. A fronteira final para qualquer ameaça possível no seu sistema computacional.** Como detecção de vírus baseada em análise de código nem sempre apresenta resultado satisfatório, o BitDefender tem implementado uma proteção baseada em comportamento, providenciando segurança contra novas ameaças ainda desconhecidas.

Estes são **os custos** que organizações querem evitar e o que os produtos são desenvolvidos para prevenir:

- Ataques de worms
- Perda de comunicação devido a e-mails infectados
- Sobrecarga de e-mails
- Limpeza e recuperação de sistemas
- Perda de produtividade por indisponibilidade dos sistemas
- Invasão, e acesso não autorizado que causam prejuízos

Algumas **melhorias e benefícios** podem ser alcançados usando o pacote de segurança do BitDefender:

- Aumento de disponibilidade da rede ao impedir códigos maliciosos de se espalharem (exemplo.: Nimda, Cavalos de tróia, DDoS).
- Protégé usuários remotos de ataques.
- Reduz custos administrativos e implementação agilizada através das capacidades de gerenciamento do BitDefender Enterprise.
- Impede a infecção de malware através de e-mail, usando uma proteção de e-mail do BitDefender no gateway da empresa. Bloqueia temporariamente ou permanentemente conexões não autorizadas, vulneráveis e pesadas.

## 2.2. Data Security Division

Desde o começo, o departamento Data Security Division da SOFTWIN's trata de proteção de dados de uma maneira específica, com a primeira atualização inteligente, não requerendo nenhuma intervenção do usuário, o primeiro gerenciamento remoto de antivírus através da tecnologia WAP ou o primeiro firewall pessoal a ser integrado

ao mecanismo antivírus para prover total resposta aos complexos problemas de ameaças de segurança atuais.

Nascido para prover completa segurança de dados em nível crítico, a Data Security Division tem como missão garantir os sistemas contra vírus de computador, pesquisa de vírus e desenvolver novas tecnologias para monitorar todas as possíveis maneiras de infecção e para educar o público sobre os perigos dos vírus de computador.

As soluções de segurança BitDefender satisfazem os requisitos de proteção do ambiente atual de negócios.

## 2.3. SOFTWIN

A SOFTWIN tem a matriz localizada em Bucareste e é líder em desenvolvimento de soluções e serviços complexos em software na Romênia.

A SOFTWIN tem como foco prover soluções e serviços de software que possibilitam empresas em rápida ascensão solucionar desafios críticos de negócios e capitalizar novas oportunidades.

A SOFTWIN possibilita empresas em focar em seu negócio primário e expandir para novos mercados, terceirizando atividades de negócios secundários.

A SOFTWIN emprega mais de 500 profissionais altamente qualificados e experientes em desenvolver soluções e serviços.

Desde sua criação em 1990, a receita anual da SOFTWIN's tem crescido em média +30%.

A SOFTWIN tem 4 divisões, que também definem as principais linhas de negócios da empresa:

- CRM
- Business Information Solutions
- eContent Solutions
- Data Security Solutions

A SOFTWIN provê serviços e soluções para clientes no mundo todo. Mais de 90% da receita da empresa é alcançada através de exportações para os EUA e a Comunidade Européia.

Usando tecnologias de última geração, a SOFTWIN desenvolveu mais de 500 projetos de software, mais de 3.500 projetos de estruturação de conteúdo para parceiros internacionais, tendo mais de 43 milhões de usuários de soluções de segurança de

dados em 80 países do mundo e mais de 1.500.000 clientes atendidos anualmente por serviços de CRM.

# 3. BitDefender 9 Standard

O **BitDefender 9 Standard** é uma poderosa ferramenta antivírus com funcionalidades que suprem sua necessidade de segurança. A facilidade de uso e as atualizações automáticas fazem do **BitDefender 9 Standard** um produto de antivírus no estilo 'instale e esqueça'.

## 3.1. Antivírus

A missão do módulo Antivírus é assegurar a detecção e remoção de todos os vírus em ação. O BitDefender Antivirus usa motores de análise robustos, certificados por ICSA Labs, Virus Bulletin, Checkmark, CheckVir e TÜV.

**B-HAVE.** Behavioral Heuristic Analyzer in Virtual Environments (B-HAVE) emula um computador-dentro-de-um-computador vistual onde pedaços de software são executados para que seja possível a análise contra comportamento potencial de malware. Esta tecnologia proprietária do BitDefender representa uma nova camada de segurança que protege o sistema operacional contra vírus desconhecidos através da detecção de pedaços de códigos maliciosos para as quais as assinaturas ainda não foram identificadas.

**Proteção Antivírus&Antispyware Permanente.** Os novos e aprimorados mecanismos de verificação BitDefender verificam e desinfectam arquivos infectados no acesso, minimizando a perda de dados. Documentos infectados podem agora ser recuperados ao invés de serem apagados.

**Proteção de Aplicativos Peer-2-Peer.** Verifica por vírus que se espalham via aplicativos de mensagens instantâneas e compartilhamento de arquivos.

**Análise e Limpeza de Spyware.** O BitDefender pode analisar o seu sistema, ou parte dele, contra ameaças spyware conhecidas. A análise usa uma base de dados de assinaturas spyware atualizada constantemente.

**Total proteção de e-mail.** O aplicativo roda no nível do protocolo POP3, bloqueando qualquer mensagem de e-mail infectada, não importando qual o cliente de e-mail usado (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat, etc), sem nenhuma configuração adicional.

## 3.2. Outros Recursos

**Autualizações de Hora em Hora.** Sua cópia do BitDefender será atualizada 24 vezes por dia através da Internet, diretamente ou através de um Servidor Proxy. O produto será capaz de auto-reparação se necessário, através de download dos arquivos danificados ou ausentes por servidores BitDefender. Usuários com uma licença BitDefender têm o benefício de atualizações gratuítas de assinaturas de vírus e spyware e atualizações gratuítas do produto.

**Suporte 24/7.** Oferecido on-line por representantes qualificados e uma base de dados on-line com respostas para perguntas freqüentes.

**Rescue Disk. BitDefender 9 Standard** é distribuído em um CD executável CD (baseado em LinuxDefender), que pode ser usado para desinfectar um sistema sem iniciar o disco rígido.

# 4. Módulos do BitDefender

**BitDefender 9 Standard** contém os módulos: **Geral**, **Antivírus** e **Atualização**.

## 4.1. Módulo Geral

O BitDefender vem totalmente configurado para segurança máxima.

Informações essenciais de status sobre todos os módulos BitDefender são exibidas no módulo Geral. Aqui você pode registrar o seu produto e pode configurar o comportamento geral do BitDefender.

## 4.2. Módulo Antivírus

O BitDefender protege seu sistema contra a infecção de vírus verificando seus arquivos, mensagens de e-mail, downloads e qualquer outro conteúdo quando entrar no sistema. Pelo módulo antivírus você tem acesso a todas as opções e recursos de antivírus do BitDefender.

A proteção contra vírus é dividida em duas categorias:

- Verificação no-acesso - Previne novos vírus de entrar em seu sistema. Isso também é chamado de virus shield – Os arquivos são analisados quando o usuário os acessa. O BitDefender irá, por exemplo, verificar um documento de Word por vírus quando você o abrir, e uma mensagem de e-mail quando você recebê-la. O BitDefender verifica arquivos "enquanto você os utiliza" – no-acesso.

- Verificação solicitada - Detecta vírus já residentes em seu sistema. Essa é a clássica verificação iniciada pelo usuário – você escolhe qual unidade, pasta ou arquivo o BitDefender deve verificar, e o BitDefender verifica – solicitado.

## 4.3. Módulo Atualização

Novos vírus são achados e identificados todos os dias. É por isso que é muito importante manter o BitDefender atualizado com as últimas assinaturas de vírus. Por padrão, o BitDefender procura automaticamente por atualizações a cada hora.

Atualizações vêm das seguintes formas:

- **Atualização dos mecanismos antivírus** - conforme novas ameaças aparecem, os arquivos contendo as assinaturas de vírus devem ser atualizados para assegurar proteção permanente atualizada contra eles. Esta atualização também é conhecido como **Atualização de Definições de Vírus**.

- **Atualização do produto** - quando uma nova versão do produto é lançada, novos recursos e técnicas de verificação são introduzidos para aprimorar a performance do produto. Esta atualização também é conhecido como **Atualização de versão do produto**.

Além disso, do ponto de vista de intervenção do usuário, podemos contar:

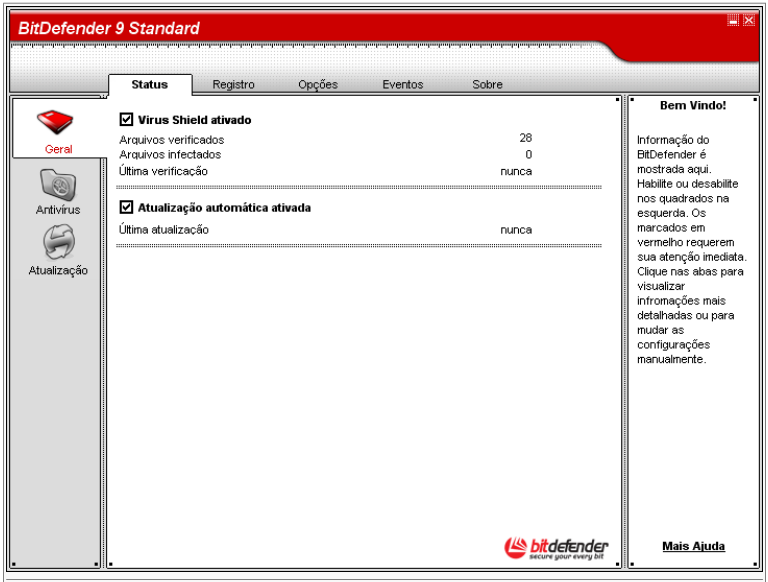
- Atualização automática - o antivírus cantata automaticamente os servidores da BitDefender para verificar se existe uma nova atualização. Se for o caso, o BitDefender será atualizado automaticamente. A atualização automática pode ser feita a qualquer hora clicando **Atualizar agora** do módulo Atualização.
- Atualização manual - você deve baixar e instalar as últimas definições de vírus e spyware manualmente.

# Console de Gerenciamento

# 5. Visão Geral

**BitDefender 9 Standard** foi desenvolvido com um console de gerenciamento centralizado, que permite a configuração das opções de proteção para todos os módulos BitDefender. Em outras palavras, é o bastante abrir o console de gerenciamento para ter acesso a todos os módulos: **Antivírus** e **Atualização**.

Para acessar a console de gerenciamento, use o menu Iniciar do Windows, seguindo o caminho : **Iniciar** -> **Programas** -> **BitDefender 9** -> **BitDefender 9 Standard** ou mais rapidamente, clique duas vezes no **Ícone BitDefender** na barra do sistema.




Console de gerenciamento

No lado esquerdo do console de gerenciamento você pode ver o seletor de módulos:

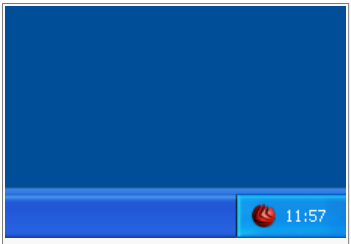
- Geral - nesta seção você pode ver um sumário de todas as principais configurações do BitDefender, detalhes de produtos e informação sobre contato. Aqui você também pode registrar o produto.

- Antivírus - nesta seção você pode configurar o módulo de **Antivírus**.
- Atualização - nesta seção você pode configurar o módulo de **Atualização**.

No lado direito da console de gerenciamento você pode ver a informação relacionada a seção que você se encontra. A opção **Mais Ajuda**, no canto inferior direito, abre o arquivo de **Ajuda**.

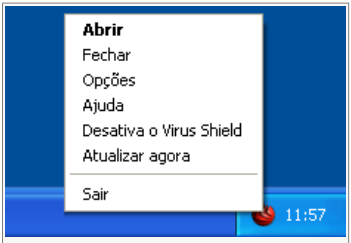
## 5.1. Barra de tarefas

Quando o console é minimizado, um ícone aparecerá barra de tarefas:



Barra de tarefas

Se você der um duplo clique nesse ícone, o console de gerenciamento será aberto.



Menu contextual

Além disso, clicando com o botão direito nele, um menu se abrirá contendo as seguintes opções.

- **Mostrar** - abre o console de gerenciamento.
- **Fechar** - minimiza o console de gerenciamento para a área de notificação.
- **Opções** - abre a seção de Configurações na console de gerenciamento.
- **Ajuda** - abre a documentação eletrônica.
- **Ativa / Desativa o Virus Shield** - ativa/desativa a proteção por acesso.
- **Atualizar agora** - realiza uma atualização imediata.

- **Sair** - fecha o aplicativo. Selecionando essa opção, o ícone da área de notificação desaparecerá e para acessar o console de gerenciamento, você terá que abri-lo de novo a partir do menu Iniciar.

Nota

- O ícone se tornará preto, se você desabilitar um ou mais módulos do BitDefender. Desta forma você saberá se alguns módulos estão desabilitados sem abrir a console de gerenciamento.
- O ícone irá piscar quando uma atualização estiver disponível.

## 5.2. Barra de atividade de verificação

A **Barra de atividade de verificação** é uma visualização gráfica da atividade de verificação em seu sistema.

Barra de atividade

As barras verdes (a zona de **Arquivos**) mostram o número de arquivos verificados por segundo, em escala de 0 a 50.

Nota

A **Barra de atividade de análise** irá lhe notificar quando o Virus Shield for desabilitado com uma cruz vermelha sobre a área correspondente (**Arquivos**). Desta forma você saberá se está protegido sem abrir a console de gerenciamento.

Quando você não quiser mais a visualização gráfica, basta clicar nela com o botão direito e escolher **Ocultar**.

Nota

Para ocultar completamente esta janela, retire a opção **Habilitar barra de atividade** (no módulo **Geral**, seção Opções).

# 6. Módulo Geral

A seção **Geral** deste manual do usuário contém os seguintes tópicos:

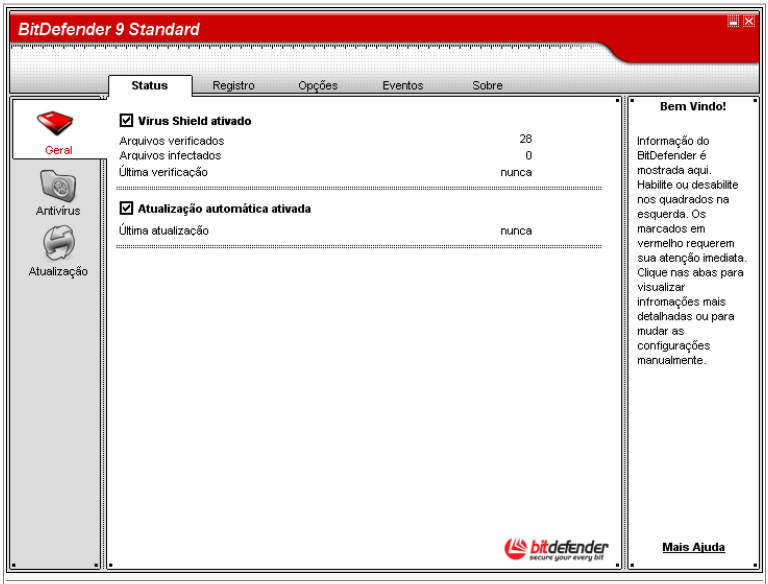
- Informação geral
- Registro do Produto
- Configurações da console de gerenciamento
- Eventos
- Sobre

**Nota**

Para mais detalhes correspondentes ao módulo do **Geral** verifique a descrição do "*Módulo Geral*" (p. 33).

## 6.1. Informação geral

Para acessar esta seção clique na aba **Status** no módulo **Geral**.




Informação geral

Aqui você pode rever informações sobre o status do produto.

Ajustando ou removendo as marcas das caixas de seleção, você pode ativar ou desativar os recursos principais do BitDefender.

**Atenção**
Itens marcados em vermelho requerem sua atenção imediata.

## 6.1.1. Virus Shield

Fornece proteção continua e em tempo-real contra vírus e outras ameaças. O número de arquivos rastreados, arquivos infectados e a data do ultimo rastreamento são disponibilizadas.

**Nota**
Para prevenir seu computador de ser infectado por vírus, mantenha o **Virus Shield** ativado.

**Atenção**
É altamente recomendado que você execute uma verificação completa pelo menos uma vez por semana. Para executar uma verificação completa do sistema, acesse o **módulo Antivírus**, seção Verificação, marque **Unidades locais** e clique em **Verificar**.

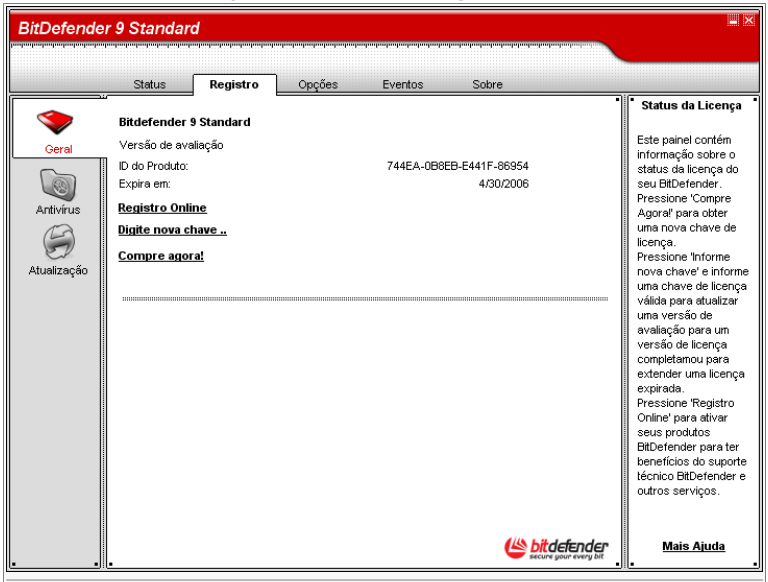
### 6.1.2. Atualização Automática

Novos vírus são encontrados e identificados todos os dias. É por isso que é muito importante manter o BitDefender atualizado com as últimas assinaturas de vírus. Ele exibe a data da última atualização.

**Nota**
Para proteger seus dados importantes, o BitDefender pode realizar atualizações automáticas. Mantenha a opção **Atualização Automática** ativada.

## 6.2. Registro do Produto

Para acessar esta seção clique na aba **Registro** no módulo **Geral**.


BitDefender 9 Standard
Status
Registro
Opções
Eventos
Sobre
Geral
Antivírus
Atualização
Bitdefender 9 Standard
Versão de avaliação
ID do Produto:
744EA-0B8EB-E441F-86954
Expira em:
4/30/2006
Registro Online
Digite nova chave ..
Compre agora!
Status da Licença
Este painel contém informação sobre o status da licença do seu BitDefender.
Pressione 'Compre Agora!' para obter uma nova chave de licença.
Pressione 'Informe nova chave' e informe uma chave de licença válida para atualizar uma versão de avaliação para um versão de licença completamou para extender uma licença expirada.
Pressione 'Registro Online' para ativar seus produtos BitDefender para ter benefícios do suporte técnico BitDefender e outros serviços.
Mais Ajuda
Registro do Produto

Essa seção contém informações sobre o status de suas licenças BitDefender. Aqui você pode registrar o produto e ver a data em que ele expira.

O produto vem com uma chave de registro válida por 30 dias. No término desse período de avaliação, se você quiser adquirir a licença do produto, terá que ter uma nova chave de licença. Clique em **Compre agora!** para adquirir uma nova **Chave de Licença** da loja on-line BitDefender.

Clique em **Registro on-line** para ativar o seu produto BitDefender para ter benefício do suporte técnico BitDefender e outros serviços.

Para modificar a chave de licença padrão, clique em **Digite nova chave...**. A seguinte janela abrirá:

BitDefender 9 Standard - Registro
Você está prestes a registrar a versão completa do BitDefender.
Por favor informe o seu número de série. Você pode achá-lo em:
- Cartão de registro do produto
- Etiqueta do CD-ROM
Se você não tem um número de série, por favor entre em contato com: sales@bitdefender.com
Série:
Registro
Cancelar
Registro

Digite a chave de licença no campo **Série**. Clique em **Registro** para finalizar o processo de registro.

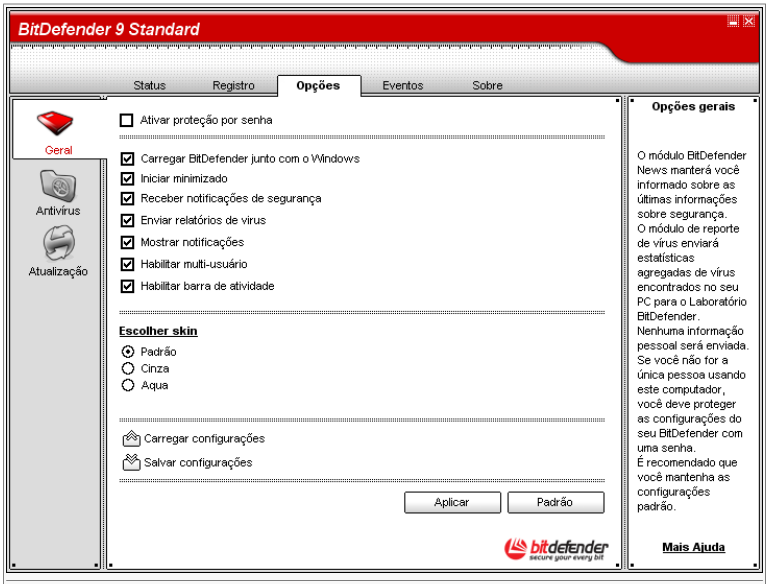
Se você errar o número da licença, terá que digitá-lo novamente.

Se você digitar uma licença válida uma mensagem de sucesso aparecerá.

Agora, na seção **Registro** você pode ver a data em que expira a nova chave de licença.

## 6.3. Configurações da console de gerenciamento

Para acessar esta seção clique na aba **Opções** no módulo **Geral**.




Configurações da console de gerenciamento

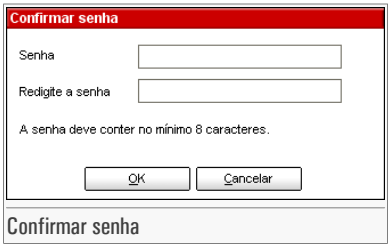
Aqui você pode ajustar o comportamento integral do BitDefender. Por padrão, o BitDefender é carregado na inicialização do Windows e então roda minimizado na área de notificação.

As seguintes opções estão disponíveis:

- **Ativar proteção por senha** - ativa a inserção de uma senha para proteger a configuração do BitDefender;

  Nota
  Se você não é a única pessoa a usar esse computador, é recomendado que você proteja suas configurações do BitDefender com uma senha.

  Se você selecionar esta opção, a próxima janela aparecerá:



Confirmar senha

Insira a senha no campo **Senha**, re-digite no campo **Redigite a senha** e clique em **OK**.

De agora em diante, se você quiser mudar as opções de configuração do BitDefender, terá que digitar a senha.

**Importante**
Se você esqueceu a senha, terá que reparar o produto para modificar a configuração do BitDefender.

- **Carregar BitDefender junto com o Windows** - inicia automaticamente o BitDefender na inicialização do sistema.

**Nota**
Nós recomendamos que você mantenha esta opção selecionada.

- **Iniciar minimizado** - minimiza o console de gerenciamento do BitDefender após ser carregado no sistema. Apenas o ícone BitDefender va aparecerá na área de notificação.
- **Receber notificações de segurança** - de tempos em tempos recebe notificações de segurança com relação a novas epidemias de vírus, enviadas pelo servidor BitDefender.
- **Enviar relatórios de vírus** - envia a BitDefender relatórios com os vírus identificados em seu computador. Isso nos ajuda a manter controle de epidemias de vírus.

  O relatório não contém dados confidenciais, tais como seu nome, endereço de IP ou outros, e não será usado para propósitos comerciais. A informação fornecida conterá apenas o nome do vírus e será usada somente para criar estatísticas.
- **Mostrar notificações** - mostrar janelas pop-up a respeito do status do produto.

- **Habilitar multi-usuário** - permite que outros usuários usem o BitDefender de forma personalizada.

**Nota**
Esta opção só pode ser habilitada ou desabilitada por usuários com poderes administrativos na máquina local.

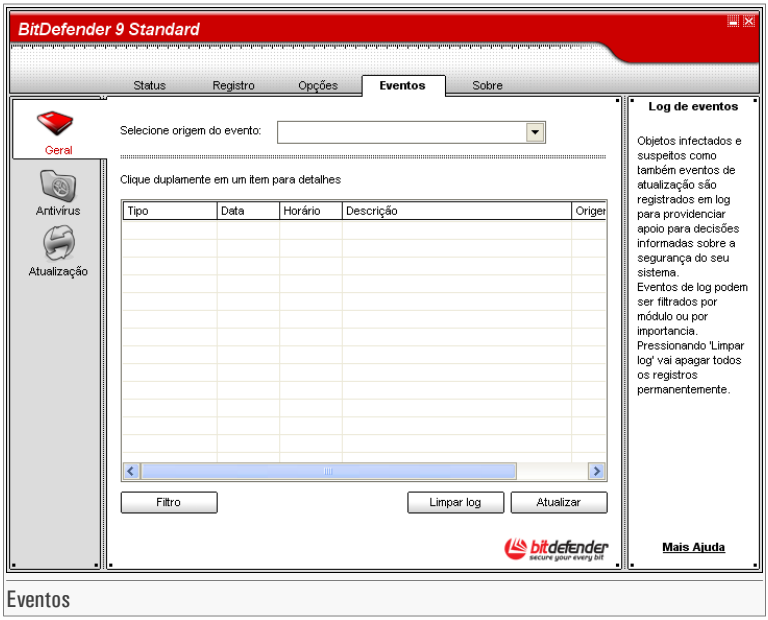
- **Habilitar barra de atividade** - habilita/desabilita " *Barra de atividade de verificação* " (p. 39).
- **Escolher Skin** - permite a você selecionar a cor do console de gerenciamento. O skin representa uma imagem de fundo da interface. Para selecionar um skin diferente, clique na cor correspondente.

Use os botões **Salvar Configurações** / **Carregar Configurações** para salvar/carregar as configurações que você fez para o BitDefender em um local específico. Desta forma você pode usar as mesmas configurações depois de reinstalar ou reparar seu produto BitDefender.

Clique em **Aplicar** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.

## 6.4. Eventos

Para acessar esta seção clique na aba **Eventos** no módulo **Geral**.




Nesta seção todos os eventos gerados pelo BitDefender são mostrados.

Existem 3 tipos de eventos: **Informação**, **Aviso** e **Crítico**.

Exemplos dos eventos:

- **Informação** - quando um e-mail é verificado;
- **Aviso** - quando um arquivo suspeito é detectado;
- **Crítico** - quando um arquivo infectado é detectado.

Para cada evento as seguintes informações são oferecidas: a data e o horário em que o evento ocorreu, uma pequena descrição e sua fonte (**Antivírus** ou **Atualização**). Clique duplamente em um evento para ver suas propriedades.

Você pode filtrar estes eventos de duas formas (por tipo ou por fonte):

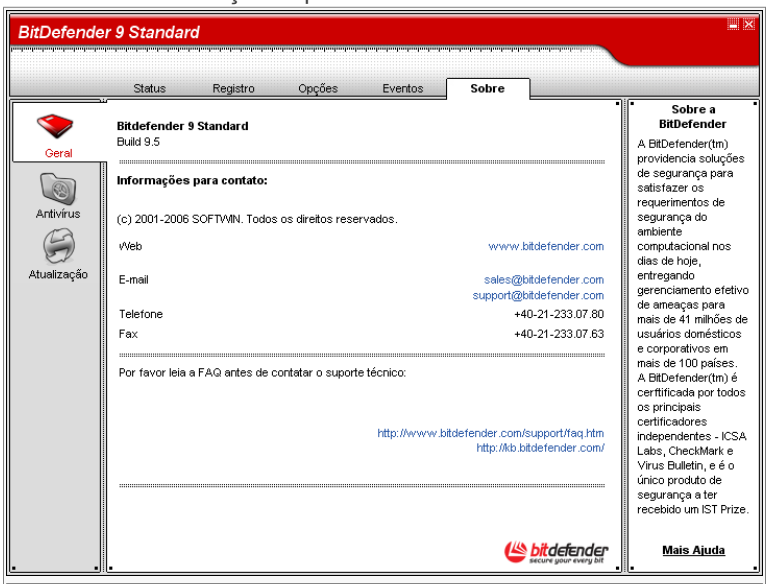
- Clique em **Filtro** para selecionar que tipos de eventos a serem mostrados.
- Selecione a fonte do evento através do menu.

Se o console de gerenciamento estiver aberto na seção **Eventos** e ao mesmo tempo um evento ocorrer você deve clicar em **Atualizar** para ver este evento.

Para apagar todos os eventos da lista clique em **Limpar log**.

## 6.5. Sobre

Para acessar esta seção clique na aba **Sobre** no módulo **Geral**.


BitDefender 9 Standard
Status
Registro
Opções
Eventos
Sobre
Geral
Antivirus
Atualização
Bitdefender 9 Standard
Build 9.5
Informações para contato:
(c) 2001-2006 SOFTWIN. Todos os direitos reservados.
Web
www.bitdefender.com
E-mail
sales@bitdefender.com
support@bitdefender.com
Telefone
+40-21-233.07.80
Fax
+40-21-233.07.63
Por favor leia a FAQ antes de contatar o suporte técnico:
http://www.bitdefender.com/support/faq.htm
http://kb.bitdefender.com/
Sobre a BitDefender
A BitDefender(tm) providencia soluções de segurança para satisfazer os requerimentos de segurança do ambiente computacional nos dias de hoje, entregando gerenciamento efetivo de ameaças para mais de 41 milhões de usuários domésticos e corporativos em mais de 100 países. A BitDefender(tm) é certtificada por todos os principais certificadores independentes - ICSA Labs, CheckMark e Virus Bulletin, e é o único produto de segurança a ter recebido um IST Prize.
Mais Ajuda

Informação geral

Nessa seção você pode achar as informações de contato e detalhes do produto.

A BitDefenderTM fornece soluções de segurança para satisfazer as necessidades de proteção do ambiente de informática de, oferecendo gerenciamento efetivo de ameaças para mais de 43 milhões de usuários domésticos e corporativos em mais de 100 países.

BitDefenderTM é certificado pelos maiores inspetores independentes - **ICSA Labs**, **CheckMark** e **Virus Bulletin** e é o único produto de segurança a ter recebido um **IST**.

# 7. Módulo do Antivírus

A seção **Antivírus** deste manual do usuário contém os seguintes tópicos:

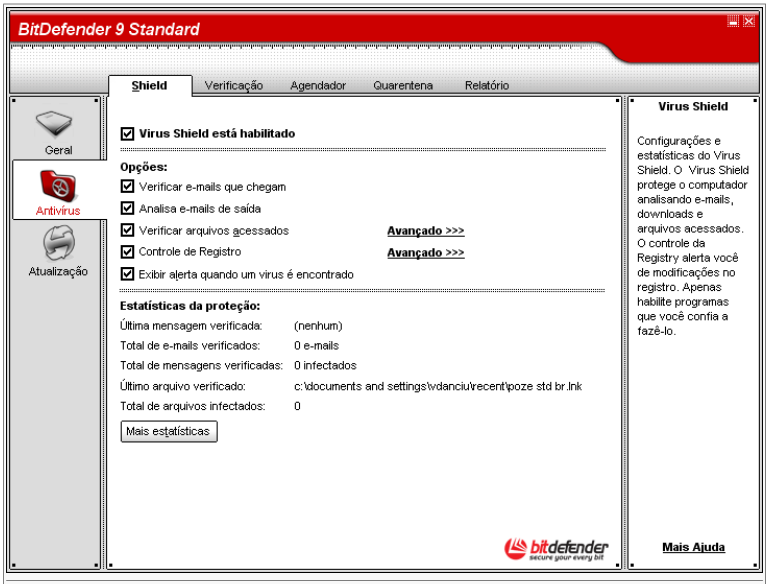
- Verificação no-acesso
- Verificação solicitada
- Verificação agendada
- Quarentena
- Relatório

**Nota**

Para mais detalhes correspondentes ao módulo do **Antivírus** verifique a descrição do "*Módulo Antivírus*" (p. 33).

## 7.1. Verificação no-acesso

Para acessar esta seção clique na aba **Shield** do módulo de **Antivírus**.


BitDefender 9 Standard
Shield
Verificação
Agendador
Quarentena
Relatório
Geral
Antivírus
Atualização
Virus Shield está habilitado
Opções:
Verificar e-mails que chegam
Analisa e-mails de saída
Verificar arquivos acessados
Avançado >>>
Controle de Registro
Avançado >>>
Exibir alerta quando um vírus é encontrado
Estatísticas da proteção:
Última mensagem verificada: (nenhum)
Total de e-mails verificados: 0 e-mails
Total de mensagens verificadas: 0 infectados
Último arquivo verificado: c:\documents and settings\vdanciu\recent\poze std br.lnk
Total de arquivos infectados: 0
Mais estatísticas
Virus Shield
Configurações e estatísticas do Virus Shield. O Virus Shield protege o computador analisando e-mails, downloads e arquivos acessados. O controle da Registry alerta você de modificações no registro. Apenas habilite programas que você confia a fazê-lo.
Mais Ajuda
Virus Shield

Nesta seção você pode configurar o **Virus Shield** e você pode ver informações sobre a sua atividade. O **Virus Shield** protege seu computador monitorando mensagens de e-mail, downloads e todos os arquivos acessados.

**Nota**
Para prevenir vírus de infectar seu computador mantenha o **Virus Shield** ativado.

No canto inferior da seção você pode ver as estatísticas do **Virus Shield** sobre arquivos e mensagens de e-mail. Clique em **Mais estatísticas** se você quiser ver uma janela mais explicada sobre essas estatísticas.

## 7.1.1. Controle de Registro

Uma parte muito importante do sistema operacional Windows é chamada de **Registro**. É aqui que o Windows mantém suas configurações, programas instalados, informações de usuário e informações do gênero.

O **Registro** é também usado para definir quais programas deverão ser iniciados automaticamente quando o Windows inicia. Vírus costumam usar isso para serem executados automaticamente quando o usuário reinicia seu computador.

O **Controle de Registro** fica de olho no Registro do Windows – Isso é útil também para detectar Trojans. Você será alertado sempre que um programa tentar modificar uma entrada de registro para ser executado na inicialização do Windows.

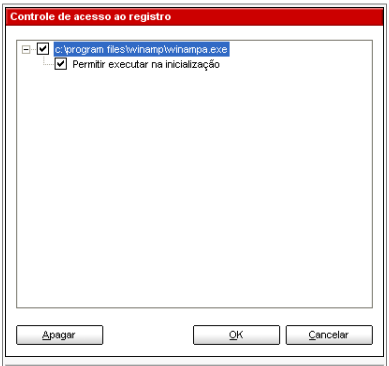
Alerta do Registro

Você pode negar as modificações clicando em **Não** ou permiti-las clicando em **Sim**.

Se você quer que o BitDefender lembre de sua resposta, você deve selecionar: **Lembrar dessa resposta**.

**Nota**
Suas respostas serão a base da lista de regras.

Se você quer ver a lista de entradas do registro, clique **Avançado >>>** correspondendo a **Controle de Registro**.



Controle de acesso ao registro

Para cada aplicativo um pequeno menu expansível será criado, contendo todas as modificações do registro.

Para apagar uma entrada do registro, apenas selecione-a e clique em **Apagar**. Para desativar temporariamente uma entrada do registro sem apagá-la, desmarque a caixa de seleção ao lado.

**Nota**
O BitDefender normalmente irá alertá-lo quando você instalar novos programas que precisam rodar após a próxima inicialização de seu computador. Na maioria dos casos, esses programas são legítimos e podem ser confiados.

## 7.1.2. As opções mais importantes

Para selecionar uma opção, apenas clique com o mouse na caixa de seleção correspondente.

- **Verificar e-mails que chegam** - verifica todos os e-mails de saída que chegam.
- **Analisa e-mails de saída** - verifica todos os e-mails de saída.
- **Verificar arquivos acessados** - verifica todos os arquivos acessado.
- **Exibir alerta quando um vírus é encontrdo** - uma janela de alerta será exibida quando um vírus for encontrado em um arquivo ou e-mail.

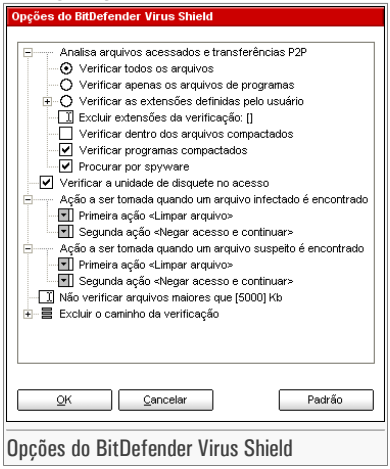
  Para um arquivo infectado a janela de alerta conterá o nome do vírus, a localização, a ação a ser tomada e a referência onde achar mais informação. Para um e-mail infectado a janela de alerta também conterá informação sobre o remetente e o destinatário.

  Caso um arquivo suspeito é detectado você pode executar um assistente que o ajudará a mandar este arquivo para o Laboratório BitDefender para uma melhor

análise. Você pode digitar o seu endereço de e-mail para receber informação sobre este relatório.

## 7.1.3. Outras opções

Usuários avançados podem desejar tirar vantagem das configurações de análise que o BitDefender oferece. O analisador pode ser ajustado para pular certas extensões de arquivo, pastas e arquivos que você saiba que não oferecem perigo. Clique em **Avançado>>>** correspondendo a **Verificar arquivos acessados** para explorar essas configurações.



Opções do BitDefender Virus Shield

Clique na caixa com "+" para abrir uma opção ou na caixa com "-" para fechar uma opção.

Você pode observar que algumas opções de verificação, embora tenham o sinal de "+", não podem ser abertas. A razão é que essas opções ainda não estão selecionadas. Você observará que, se você selecioná-las, elas poderão ser abertas.

- **Analisa arquivos acessados e transferência P2P** - para verificar os arquivos acessados e comunicação entre programas de mensagens instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Selecione também o tipo de arquivos a serem verificados.

  As seguintes opções estão disponíveis:

| Opção | Descrição |
|---|---|
| **Verificar todos os arquivos** | Todos os arquivos acessados serão verificados, não importando o tipo. |
| **Verificar apenas os arquivos de programas** | Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes |

| Opção | Descrição |
|---|---|
| | extensões: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws. |
| **Verificar as extensões definidas pelo usuário** | Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";". |
| **Excluir extensões da verificação** | Os arquivos com as extensões especificadas pelo usuário NÃO serão verificados. Essas extensões devem ser separadas por ";". |
| **Verificar dentro dos arquivos compactados** | Arquivos de backup acessados também serão verificados. Com essa opção ativada, o computador ficará lento. |
| **Verificar programas compactados** | Todos os programas compactados serão verificados. |
| **Procurar por spyware** | Rastrea por aplicativos spyware. Estes arquivos serão tratados como arquivos infectados. Programas que incluem componentes adware podem parar de funcionar se esta opção estiver habilitada. |

- **Verificar a unidade de disquete no acesso** - verifica a unidade de disquete quando acessada.
- **Ação a ser tomada se um arquivo infectado é encontrado** - escolha na lista a primeira ação a tomar em arquivos infectados. O BitDefender permite escolher duas ações caso encontre um arquivo infectado.

  Você pode escolher uma das seguintes opções:

| Ação | Descrição |
|---|---|
| **Negar acesso e continuar** | Caso um arquivo infectado seja detectado, o acesso a ele será negado. |

| Ação | Descrição |
|---|---|
| **Limpar arquivo** | Para desinfectar o arquivo infectado. |
| **Apagar arquivo** | Apaga o arquivo infectado imediatamente, sem avisar. |
| **Mover o arquivo para a quarentena** | Os arquivos infectados são movidos para a quarentena. |

- **Segunda ação a ser tomada se a primeira falhar** - selecione através do menu a segunda ação a ser tomada em arquivos infectados, caso a primeira ação falhe.

  Você pode escolher uma das seguintes opções:

| Ação | Descrição |
|---|---|
| **Negar acesso e continuar** | Caso um arquivo infectado seja detectado, o acesso a ele será negado. |
| **Apagar arquivo** | Apaga o arquivo infectado imediatamente, sem avisar. |
| **Mover o arquivo para a quarentena** | Os arquivos infectados são movidos para a quarentena. |

  As mesmas ações para arquivos infectados estão disponíveis para arquivos suspeitos.

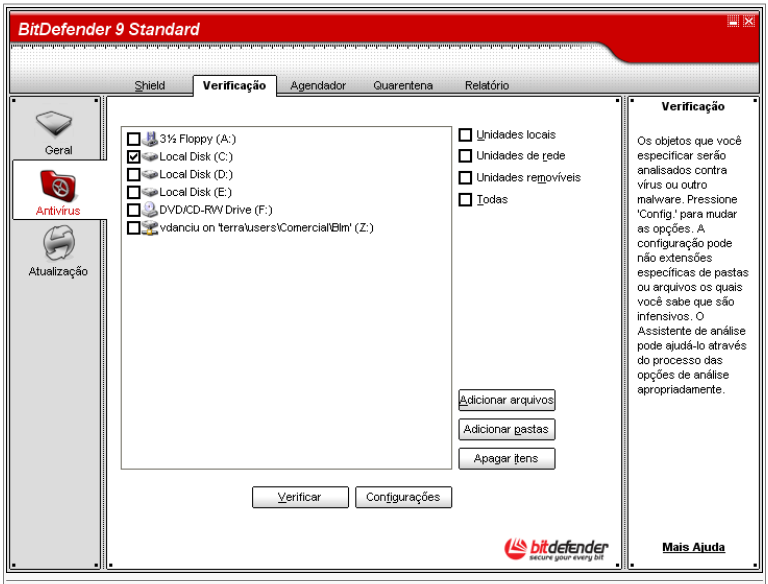
- **Não verificar arquivos maiores que** - digite o tamanho máximo dos arquivos a serem verificados. Se o tamanho for 0Kb, todos os arquivos serão verificados.

- **Excluir o caminho da verificação** - clique "+" correspondendo a esta opção para definir uma pasta que será excluída da verificação. A conseqüência disso será que uma nova opção, `Novo Item`, aparecerá. Clique na caixa correspondente ao novo item e selecione na janela de explorar a pasta que você quer excluir da verificação.

Clique em **OK** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.

## 7.2. Verificação solicitada

Para acessar esta seção clique na aba **Verificação** do módulo de **Antivírus**.



Análise de Vírus

Nesta seção você pode configurar o BitDefender para verificar seu computador.

O objetivo principal para o BitDefender é manter seu computador livre de vírus. Isso é feito primordialmente mantendo novos vírus fora de seu computador e verificando seus e-mails e novos arquivos copiados para seu sistema.

Há o risco que um vírus já esteja alojado em seu sistema, antes mesmo de você instalar o BitDefender. É por isso que é uma ótima idéia verificar seu computador contra vírus residentes após instalar o BitDefender. E é definitivamente uma boa idéia verificar seu computador freqüentemente contra vírus.

O BitDefender permite quatro tipos de verificação solicitada:

- Verificação imediata - existem uns poucos passos para seguir para verificar seu computador;
- Verificação contextual - clique com o botão direito em um arquivo ou pasta e escolha BitDefender Antivirus v9;
- Verificação Arraste &Solte - arraste e solte um arquivo ou pasta sobre a Barra de Atividade;

- Verificação agendada - você pode programar o BitDefender para verificar seu sistema contra vírus periodicamente.

## 7.2.1. Verificação imediata

Para executar uma verificação imediata, por favor siga os seguintes passos:

### Passo 1/5 - Feche todos os programas

Para que o BitDefender execute uma verificação completa, você precisará fechar todos os programas abertos. Especialmente seu cliente de e-mail (i.e. Outlook, Outlook Express ou Eudora) deve ser.

### Passo 2/5 - Assegure-se de que o BitDefender conhece os últimos vírus

Antes de executar a verificação, você deve se assegurar de que o BitDefender está atualizado com as últimas assinaturas de vírus, já que novos vírus são encontrados e identificados todos os dias. Você pode verificar quando a última atualização foi feita no canto inferior do modulo Atualização.

### Passo 3/5 - Escolha os alvos da verificação

No console de gerenciamento, entre no módulo **Antivírus** e clique na guia Verificação. Por padrão, essa seção contém uma imagem da estrutura de partições do sistema. Além disso, alguns botões e opções de verificação podem ser observados.

Essa seção contém os seguintes botões:

- **Adicionar arquivo(s)** - abre uma janela onde você pode selecionar o(s) arquivo(s) que deseja verificar.
- **Adicionar pasta(s)** - o mesmo acima, mas você selecionará que pasta(s) deseja verificar, ao invés de arquivos.

Nota
Use arrastar & soltar para incluir arquivos/pastas na lista.

- **Apagar item (ns)** - remove os arquivos/pastas que foram selecionados anteriormente na lista de objetos a serem verificados.

**Nota**
Apenas os arquivos/pastas que foram inclusos posteriormente podem ser removidos, mas não os que foram "vistos" automaticamente pelo BitDefender.

- **Configurações** - abre uma janela onde você pode especificar quais arquivos serão verificados, a ação nos arquivos infectados, geração de alertas de mensagens e gravação dos resultados da verificação em arquivos de relatórios.
- **Verificar** - inicia a verificação do sistema, levando em conta as opções selecionadas.

Além dos botões explicados acima existem algumas opções que possibilitam seleção rápida de local de verificação.

- **Unidades locais** - para verificar as unidades locais.
- **Unidades de rede** - para verificar todas as unidades da rede.
- **Unidades removíveis** - para verificar as unidades removíveis (CD-ROM, disquete, etc).
- **Todas** - para verificar todas as unidades, não importando se são locais, na rede ou removíveis.

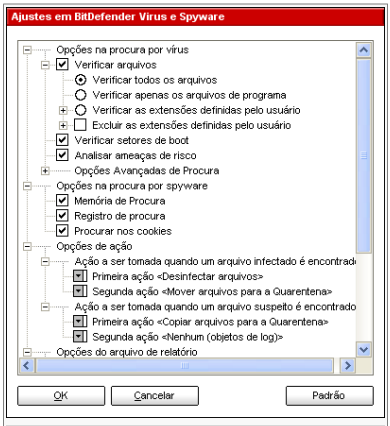
**Nota**
Se você quer verificar todo o seu computador contra vírus selecione a caixa correspondente a **Todas**.

**Importante**
Se você não está familiar com computadores, agora é hora de apenas clicar no botão **Verificar**. O BitDefender começará a verificar seu computador usando as opções padrão, que são suficientes.

## Passo 4/5 - Selecione as opções de verificação

Usuários avançados podem querer obter vantagem das opções de verificação que o BitDefender oferece. O verificador pode ser ajustado para pular extensões de arquivos, pastas ou arquivos que você sabe que são inofensivos. Isso pode reduzir drasticamente o tempo da verificação e aumentar a resposta de seu computador durante uma verificação.

Clique **Configurações** da seção Verificação para explorar estas opções.



Opções de Verificação

As opções de verificação são organizadas como um menu expansível muito parecido com o Explorer do Windows.

As opções de verificação são agrupadas em 5 categorias:

- **Opções na procura por vírus**
- **Opções na procura por spyware**
- **Opções de ação**
- **Opções do arquivo de relatório**
- **Outras opções**

**Nota**

Clique na caixa com "+" para abrir uma opção ou na caixa com "-" para fechar uma opção .

- Especifique os tipos de objetos a serem analisados (arquivos, e-mail, etc.) e outras opções. Isto é feito através da seleção de certas opções da categoria **Opções na procura por vírus**.

  As seguintes opções de detecção estão disponíveis:

| Opção | | Descrição |
|---|---|---|
| **Verificar arquivos** | **Verificar todos os arquivos** | Todos os arquivos acessados serão verificados, não importando o tipo. |

| Opção | | Descrição |
|---|---|---|
| | **Verificar apenas os arquivos de programas** | Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes extensões: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws. |
| | **Verificar as extensões definidas pelo usuário** | Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";". |
| | **Excluir as extensões definidas pelo usuário** | Os arquivos com as extensões especificadas pelo usuário NÃO serão verificados. Essas extensões devem ser separadas por ";". |
| **Verificar setores de boot** | | Para verificar o setor de boot do sistema. |
| **Analisar ameaças de risco** | | Verifica por outras ameaças que não são vírus, como dialers e adware. Estes arquivos serão tratados como arquivos infectados. Programas que incluem componentes adware podem parar de funcionar se esta opção estiver habilitada. |
| **Opções Avançadas de Procura** | **Abrir programas compactados** | Arquivos de backup acessados também serão verificados. |
| | **Abrir arquivos** | Todos os arquivos compactados serão verificados. |
| | **Abrir arquivos de e-mails** | Para verificar dentro de arquivos de e-mails. |
| | **Usar detecção heurística** | Para usar a verificação heurística dos arquivos. O objetivo da verificação heurística é detector novos vírus, baseada em certos modelos e algoritmos, antes que haja uma definição de vírus. Mensagens de alarme falso |

| Opção | | Descrição |
|---|---|---|
| | | podem aparecer. Quando um arquivo é detectado ele e classificado como suspeito. Nesses casos, recomendamos que você envie os arquivos a BitDefender Labs para serem analisados. |
| | **Detectar corpos incompletos de vírus** | Para detector corpos incompletos de vírus também. |

- Especifique o alvo de rastreamento de spywares (processos, cookies e memória). Isto é feito através da seleção de certas opções da categoria **Opções na procura por spyware**.

  As seguintes opções de detecção estão disponíveis:

| Opção | Descrição |
|---|---|
| **Memória de Procura** | Analisa a memória. |
| **Registro de Procura** | Analisa entradas do registro. |
| **Procurar nos cookies** | Analisa arquivos de cookie. |

- Especifique a ação para arquivos infectados ou suspeitos. Abra a categoria **Opções de ação** para poder ver todas as possíveis ações nestes arquivos.

  Selecione as ações a serem tomadas quando um arquivo infectado ou suspeito é detectado. Você pode especificar ações diferentes parar arquivos suspeitos e infectados. Você também pode selecionar uma segunda ação se a primeira falhar.

| Opção | Descrição |
|---|---|
| **Nenhum (objetos de log)** | Nenhuma ação será tomada em arquivos infectados. Esses arquivos aparecerão no arquivo de relatório. |
| **Perguntar ao usuário sobre ação** | Quando um arquivo infectado for encontrado, uma janela aparecerá pedindo ao usuário uma ação para aquele arquivo. Dependendo da importância daquele arquivo, você pode selecionar desinfectá-lo, isolá-lo na quarentena ou apagá-lo. |

| Opção | Descrição |
|---|---|
| **Desinfetar arquivos** | Para desinfectar os arquivos infectados. |
| **Deletar arquivos** | Para apagar arquivos infectados. |
| **Renomear arquivos** | Para mudar a extensão dos arquivos infectados. A nova extensão de arquivos infectados será `.vir`. Renomeando os arquivos infectados, a possibilidade de execução e de espalhar a infecção é removida. Ao mesmo tempo os arquivos podem ser salvos para futura análise e exame. |
| **Copiar arquivos para a quarentena** | Para copiar os arquivos infectados para a zona de quarentena. Isso significa praticamente duplicar o arquivo infectado e a cópia desse arquivo aparecerá na quarentena, mas o arquivo infectado não será movido de seu local inicial. |
| **Mover arquivos para a quarentena** | Para mover os arquivos infectados para a quarentena. |

- Especifique as opções para os arquivos de relatório. Abra a categoria **Opções de relatório** para ver todas as opções disponíveis.

| Opção | | Descrição |
|---|---|---|
| **Mostrar todos os arquivos no arquivo de relatório** | | Lista todos os arquivos verificados e seu status (infectado ou não) em um arquivo de relatório. Com essa opção ativada, o computador ficará mais lento. |
| **Criar um arquivo de relatório** | **Nome do relatório** `vscan.log` | Esse é um campo editável que permite a mudança do arquivo de relatório. Para fazer isso, você terá simplesmente que clicar nessa opção e digitar um novo nome. |
| | **Tamanho máximo do arquivo de relatório [0] KB** | Limita o tamanho do arquivo relatório. Digite o tamanho máximo do arquivo no campo correspondente. |

**Nota**

Os arquivos de relatório podem ser vistos na seção Relatório do módulo **Antivírus**.

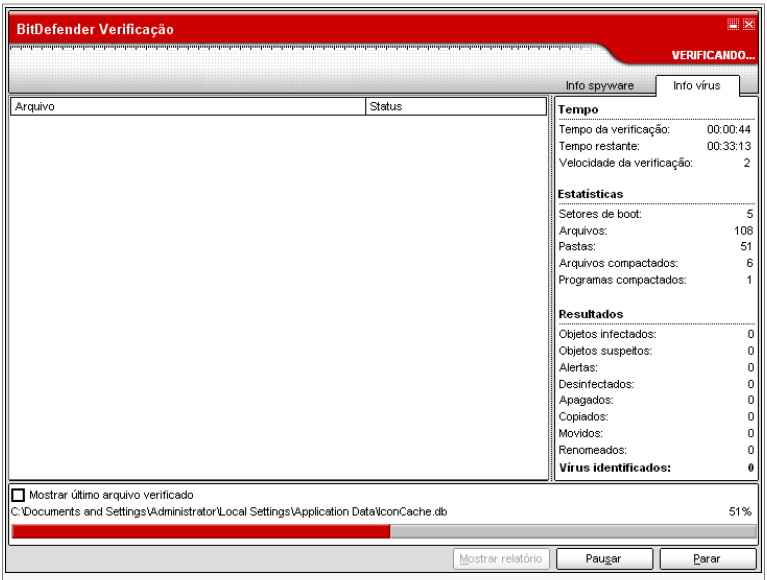
- Especifica outras opções. Abra a categoria **Outras opções** de onde você pode selecionar as seguintes opções:

| Opção | Descrição |
|---|---|
| **Executar a análise com Baixa prioridade** | Diminui a prioridade do processo de verificação. Você permitirá outros programas a executarem mais rapidamente e aumentar o tempo de verificação. |
| **Desligar o PC quando a análise for concluída** | Desliga o computador quando a verificação terminar. |
| **Enviar arquivos suspeitos para o Laboratório BitDefender** | Você será indagado a submeter todos os arquivos suspeitos parar o laboratório BitDefender após o processo de verificação for concluído. |
| **Minimizar a janela de análise no inicío para a barra de tarefas** | Minimiza a janela de verificação para a barra de tarefas. Clique duplamente no ícone BitDefender para abrir. |
| **Perguntar para reinicializar** | Se as ações requerem reinicialização, avisa usuários de reinicialização imediata. |

Clique em **OK** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.

## Passo 5/5 - Verificar por vírus

Com as opções de verificação selecionadas, tudo o que você tem que fazer é iniciar efetivamente a verificação do sistema. Para isso, apenas clique em **Verificar**. Na janela de rastreamento aparecerá:




Análise de Vírus

Enquanto rastreia, BitDefender mostrará o progresso da atividade e alertará se alguma ameaça for encontrada. Na direita você pode acessar estatísticas sobre o processo de rastreamento. Dependendo do alvo de rastreamento, informações sobre spyware e/ou vírus aparecerão. Se ambas aparecerem, clique na aba correspondente.

Escolha a caixa correspondente a **Mostrar último arquivo verificado** e apenas as informações sobre o último arquivo verificado serão visíveis.

### Nota

A verificação pode levar algum tempo, dependendo do tamanho do seu disco rígido.

Três botões estão disponíveis:

- **Parar** - uma nova janela aparecerá onde você pode finalizar a verificação do sistema. Clique **Sim**&**Fechar** para sair da janela de análise.
- **Pausar** - a verificação parará temporariamente – você pode continuar pressionando **Continuar**.

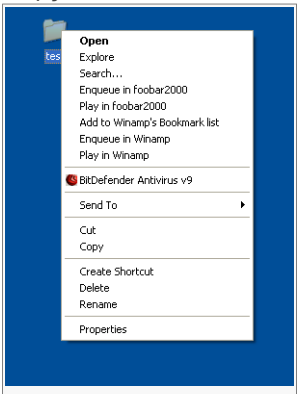
- **Mostrar relatório** - o relatório de verificação abrirá.

**Nota**
O arquivo de relatório é salvo automaticamente na seção Relatório pelo módulo **Antivírus**.

Um ícone aparecerá na barra de processos quando um processo de análise estiver em execução.

## 7.2.2. Verificação contextual

Clique com o botão direito no arquivo ou pasta que você quer verificado e selecione a opção **BitDefender Antivirus v9**.

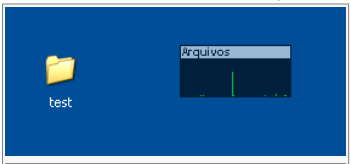


Verificação Contextual

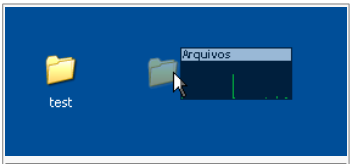
Um arquivo de relatório chamado `vscan.log` será criado e você pode vê-lo no módulo **Antivírus**, seção Relatório.

## 7.2.3. Verificação Arraste & Solte

Arraste o arquivo ou pasta que você quer verificado e solte-o sobre a **Barra de Atividade**, como nas imagens abaixo.



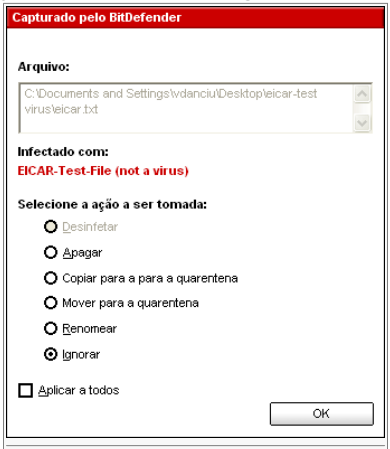
Arraste o arquivo



Solte o arquivo

Um arquivo de relatório chamado `activbar.log` será criado e você poderá vê-lo no modulo **Antivírus**, seção Relatório.

Em ambos os casos a janela de verificação aparecerá. Se um vírus é detectado, uma janela de alerta irá perguntá-lo a selecionar a ação sobre o arquivo infectado.



Ação Selecionada

Você pode ver o nome do arquivo e o nome do vírus.

Você pode selecionar uma das seguintes ações num arquivo infectado:

- **Desinfetar** - para desinfectar o arquivo infectado;
- **Apagar** - para apagar o arquivo infectado;
- **Copiar para a quarentena** - para copiar o arquivo infectado para a quarentena;
- **Mover para a quarentena** - para mover o arquivo infectado para a quarentena;
- **Renomear** - para mudar a extensão dos arquivos infectados. A nova extensão dos arquivos infectados será `.vir`.
- **Ignorar** - para ignorar a infecção. Nenhuma ação será tomada no arquivo infectado.

Se você analisar uma pasta, e desejar que a mesma ação sobre arquivos infectados seja a mesma para todos, selecione a caixa correspondente a **Aplicar a todos**.

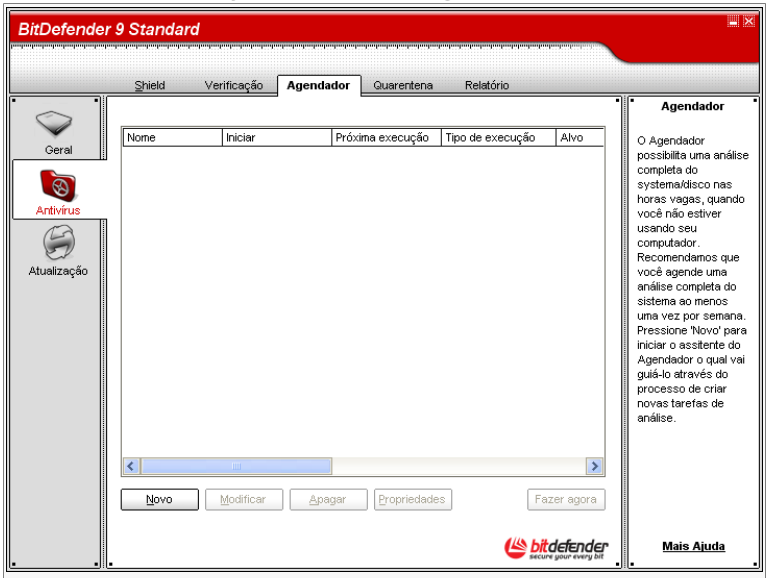
**Nota**

Se a opção **Desinfectar** não estiver habilidade, significa que o arquivo não pode ser desinfectado. A melhor escolha é isolar este arquivo para a zona de quarentena e nos envie para análise ou apague o arquivo.

Clique em **OK**.

## 7.2.4. Verificação agendada

Para acessar esta seção clique na aba **Agendador** do módulo de **Antivírus**.




Agendador

Já que a verificação leva algum tempo e funciona melhor se você fechar todos os outros programas, é melhor que você agende a verificação para quando não for utilizar o computador e ele está parado. Isso quer dizer que o usuário deve antes criar uma "tarefa", evento ou evento de verificação.

O **Agendador** contém um assistente para criar novas tarefas de verificação. Isso irá auxiliá-lo sempre que você precisar realizar alguma operação com esses eventos de verificação, não importa se for criar uma tarefa ou modificar uma existente.

A seção **Agendador** contém alguns botões para administrar as tarefas de verificação.

- **Novo** - inicia o assistente que irá guiá-lo pela criação de uma nova tarefa.
- **Modificar** - modifica as propriedades de uma tarefa já criada. Ele também iniciará o assistente.

**Nota**
Se você modificar o nome do evento, um novo evento será criado, sob o novo nome introduzido.

- **Apagar** - apaga uma tarefa selecionada.
- **Fazer Agora** - executa a tarefa selecionada.
- **Propriedades** - visualiza as propriedades da tarefa selecionada.

A tela do Agendador também contém uma lista onde todas as tarefas podem ser vistas, com seus nomes, a data da primeira execução, a data da próxima execução e o tipo da tarefa (periodicamente ou apenas mais uma vez).

Se você clicar com o botão direito em um evento agendado, um menu contextual com opções similares a aquelas descritas acima aparecerá.

**Nota**
O **Agendador** permite um número ilimitado de eventos de análise agendados.

Você pode também navegar pelos eventos usando o teclado. Pressione **Delete** para apagar os eventos selecionados, pressione **Enter** para ver as propriedades do evento selecionado ou pressione a tecla **Insert** para criar um novo evento (o assistente do Agendador aparecerá).

**Nota**
Pressione os botões de navegação para descer ou subir a página ou ir da direita para a esquerda.

Clique em **Novo** para configurar uma nova entrada no agendador. Isto irá executar o assistente do agendador, o qual vai permitir que você defina sua análise passo a passo.

## Passo 1/9 - Introdução

Introdução

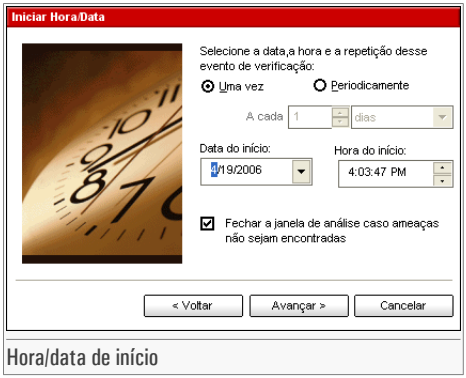
Digite o nome do novo evento no campo **Evento** e uma breve descrição no campo **Descrição do evento**.

As seguintes opções estão disponíveis:

- **Executar tarefa de análise com prioridade Baixa** - Diminui a prioridade do processo de verificação. Você permitirá outros programas a executarem mais rapidamente e aumentar o tempo de verificação.
- **Minimizar janela ao iniciar** - Minimiza a janela de verificação para a barra de tarefas. Clique duplamente no ícone BitDefender para abrir.
- **Desligar o PC quando verificação completada** - Desliga o computador quando a verificação terminar.

Clique em **Avançar** para continuar. Se você clicar em **Cancelar** uma nova janela aparecerá pedindo que você confirme sua opção de fechar o assistente ou continue.

## Passo 2/9 - Hora/data de início




Hora/data de início

Selecione a frequencia de verificação:

- **Uma vez** - executa a verificação uma vez, no determinado momento.
- **Periodicamente** - executa a verificação periodicamente, em determinados intervalos de tempo (horas, dias, semanas, meses, anos) começando com uma data e hora específica.

Se você quer que a verificação se repita após certos intervalos, selecione a caixa de seleção correspondente a **Periodicamente** e digite na caixa **A cada** o número de minutos / horas / dias / semanas / anos em que você quer repetir esse processo.

**Nota**
Você pode clicar nas setas para cima / para baixo dessa caixa para aumentar / diminuir o número de minutos / horas / dias / semanas / anos.

Escolha o intervalo – minutos, horas, dias, semanas, meses, anos –para repetir a verificação.

**Importante**
Se você optou por uma verificação repetida, ele será iniciado por um período ilimitado de tempo. Para desistir do evento, ele deve ser apagado da lista de eventos da janela do Agendador.

Se você quiser automaticamente fechar a janela de verificação se não for encontrado arquivos infectados ou, selecione a caixa respectiva a esta opção.

Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

## Passo 3/9 - Objetos alvo

Objetos alvo

Especifique os objetos que serão verificados. O alvo de rastreamento está dividido em duas categorias:

- **Análise de vírus** - rastrear por vírus.

**Nota**
Marque a caixa correspondente para definir o alvo do rastremento de vírus.

As seguintes opções estão disponíveis:

| Opção | | Descrição |
|---|---|---|
| **Boot** | | Analisa o setor de boot, para identificar os vírus de boot. |
| **Arquivos** | | Analisa arquivos. |
| | **E-mail** | Analisa arquivos de e-mails para detector vírus de e-mail. |
| | **Arquivos Antigos** | Analisa dentro de arquivos de backup. |
| | **Arquivos compactados** | Analisa arquivos compactados. |

| Opção | Descrição |
|---|---|
| **Ameaças de risco** | Verifica por outras ameaças que não são vírus, como dialers e adware. Estes arquivos serão tratados como arquivos infectados. |

- **Análise de spyware** - rastrear por aplicativos spyware.

Nota

Marque a caixa correspondente para definir o alvo do rastremento de spywares.

As seguintes opções estão disponíveis:

| Opção | Descrição |
|---|---|
| **Cookies** | Analisa arquivos de cookie. |
| **Registro** | Analisa entradas do registro. |
| **Memória** | Analisa a memória. |

Para ativar ou desativar um alvo de rastreamento marque a caixa correspondente.

Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

## Passo 4/9 - Caminho alvo

Caminho alvo

Especifique o caminho dos objetos que serão verificados. Este passo é necessário se você selecionou verificar arquivos no terceiro passo.

Essa tela na verdade é uma janela de navegação que lhe permite selecionar as partições e pastas a serem verificadas. Quando o cursor está posicionado numa pasta, o caminho complete para ela será exibido no campo posicionado abaixo dessa janela.

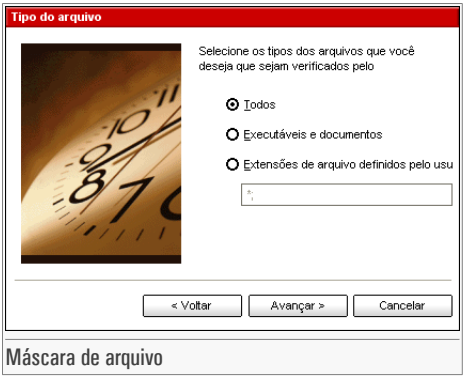
**Nota**
Clique na caixa com "+" para abrir uma opção ou a caixa "-" para fechar uma opção.

Também, para selecionar os locais a serem verificados, você pode usar as opções de seleção rápida na arte superior da janela:

- **Unidades locais** - verifica todas as unidades locais;
- **Unidades de rede** - verifica todas as unidades da rede.

Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

## Passo 5/9 - Máscara de arquivo




Máscara de arquivo

Especifique o tipo de arquivos a serem verificados. Este passo é necessário se você selecionou verificar arquivos no terceiro passo.

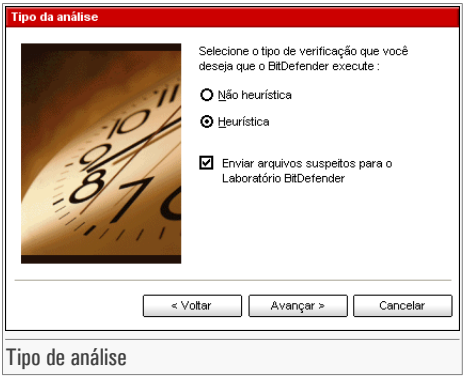
As seguintes opções estão disponíveis:

- **Todos** - para verificar todos os arquivos, não importando qual o seu tipo;
- **Executáveis e documentos** - para verificar os arquivos de programas e documentos;
- **Extensões de arquivo definidos pelo usuario** - para verificar apenas os arquivos cujas extensões estejam na lista.

**Nota**
Essas extensões devem ser separadas por ponto-e-vírgula ";".

Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

## Passo 6/9 - Tipo de análise


Tipo da análise
Selecione o tipo de verificação que você deseja que o BitDefender execute :
Não heurística
Heurística
Enviar arquivos suspeitos para o Laboratório BitDefender
< Voltar
Avançar >
Cancelar

Tipo de análise

Selecione o tipo de verificação:

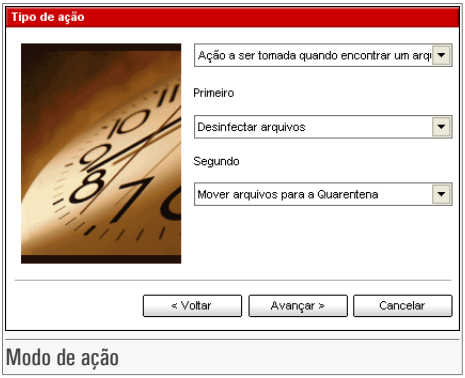
- **Não-heurística** - significa verificar os arquivos com o procedimento baseado em assinaturas de vírus conhecidos;
- **Heurística** - representa um método baseado em certos algoritmos, cujo objetivo é identificar novos vírus desconhecidos. Ocasionalmente, pode informar um código suspeito em programas normais, gerando o chamado **alarme-falso**.

Você tem a seguinte opção:

- **Enviar arquivos suspeitos para o Laboratório BitDefender** - Você será indagado a submeter todos os arquivos suspeitos parar o laboratório BitDefender após o processo de verificação for concluído.

Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

## Passo 7/9 - Modo de ação




Modo de ação

O BitDefender premite selecionar duas ações no caso de arquivos suspeitos ou infectados serem encontrados. Selecione as ações para arquivos infectados ou suspeitos.

| Ação | Descrição |
|---|---|
| **Nenhum(objetos de log)** | Nenhuma ação será tomada em arquivos infectados. Esses arquivos aparecerão no arquivo de relatório. |
| **Perguntar ao usuário sobre ação** | Quando um arquivo infectado for encontrado, uma janela aparecerá pedindo ao usuário uma ação para aquele arquivo. Dependendo da importância daquele arquivo, você pode selecionar desinfectá-lo, isolá-lo na quarentena ou apagá-lo. |
| **Desinfetar arquivos** | Para desinfectar os arquivos infectados. |
| **Apagar arquivos** | Para apagar arquivos infectados. |
| **Renomear arquivos** | Para mudar a extensão dos arquivos infectados. A nova extensão dos arquivos infectados será `.vir`. Renomeando os arquivos infectados, a possibilidade de execução e disseminação do vírus é eliminada. Ao mesmo tempo eles podem ser salvos para melhor análise. |
| **Copiar arquivos para a quarentena** | Para copiar os arquivos infectados para a zona de quarentena. Isso significa praticamente duplicar o |

| Ação | Descrição |
|---|---|
| | arquivo infectado e a cópia desse arquivo aparecerá na quarentena, mas o arquivo infectado não será movido de seu local inicial. |
| **Mover arquivos para a quarentena** | Para mover os arquivos infectados para a quarentena. Enquanto um vírus está n quarentena ele é inofensivo. |

**Nota**

Nós recomendamos que você escolha a primeira ação como **Desinfetar arquivos** e a segunda ação como **Mover arquivos para a quarentena**.

As mesmas ações para arquivos infectados estão disponíveis para arquivos suspeitos.

Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

## Passo 8/9 - Informações de Relatório

Informações do relatório
Se você desejar um arquivo de relatório, marque "Criar arquivo de relatório".
Listar todos os objetos checados
Criar arquivo de relatório
Nome do arquivo de relatório :
schedule.log
Limitar o tamanho do Relatório para
0
KB
< Voltar
Avançar >
Cancelar

Informações de Relatório

Para criar um relatório da verificação, clique em **Criar arquivo de relatório**. Nesse momento todas as outras opções para a criação de relatórios serão ativadas.

Digite o nome do relatório na caixa **Nome do arquivo de relatório**. Por padrão, seu nome é `schedule.log`. Ele conterá todas as informações sobre o progresso da verificação: o número de vírus identificados, o número de arquivos verificados, o número de arquivos desinfectados e apagados.

Você também pode limitar o tamanho do arquivo do relatório. Digite o tamanho máximo do arquivo no campo correspondente.

Se você deseja ver informações sobre todos os arquivos verificados, infectados ou não, selecione a opção **Listar todos os objetos checados**. Com essa opção ativada, o computador ficará lento.

**Nota**
Você pode ver o arquivo de relatório na seção Relatório do módulo **Antivírus**.

Clique em **Voltar** para ir para voltar ao passo anterior ou clique em **Avançar** para continuar.

### Passo 9/9 - Sumário

Resumo
Por favor veja abaixo as opções de verificação:
Iniciar: 4/19/2006 4:03:47 PM
Executar: somente uma vez
Objetivos: boot; spyware; cookies; registry; memória;
Tipos de arquivos: *;
Análise: heurística
Arquivo de relatório: schedule.log
Ação a ser tomada quando encontrar um: Desinfectar arquivos / Mover arquivos para a Quarentena
Ação a ser tomada quando encontrar um: Copiar arquivos para a Quarentena / Nenhum (objetos de log)
Desligar PC quando verificação completada: Nao
Prioridade: Prioridade
Minimizar janela ao iniciar: Sim
Enviar arquivos suspeitos para o Laboratório BitDefender: Sim
Tempo decorrido entre o fim da análise e saída: depois de 1 segundos
Analisa ameaças de risco: Sim
< Voltar
Concluir
Cancelar
Sumário

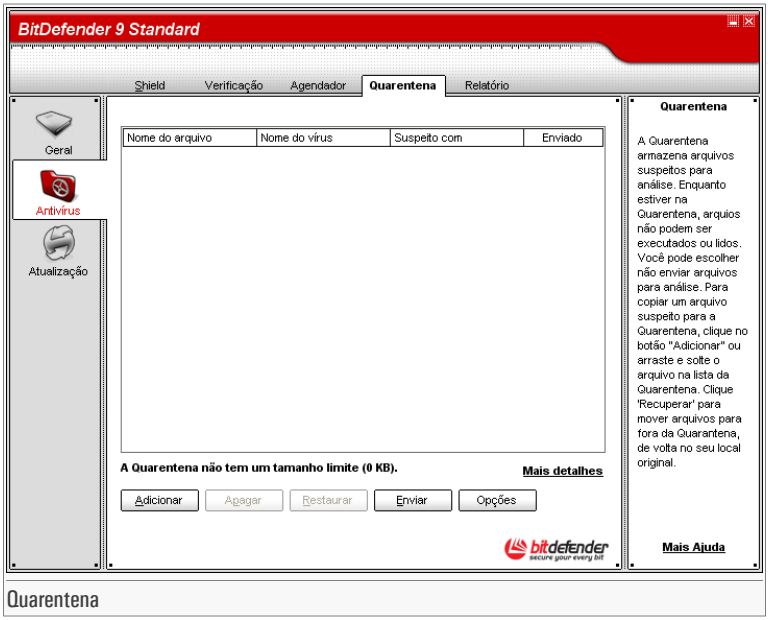
Este é o último passo do assistente. Nesta janela você pode ver todos as configurações para o novo evento de análise e você pode fazer quaisquer mudanças, retornando para os passos anteriores (**Voltar**).

Se você não quer mudar nada, clique em **Concluir**.

O novo evento aparecerá na seção Agendador.

## 7.3. Quarentena

Para acessar esta seção clique na aba **Quarentena** do módulo de **Antivírus**.


BitDefender 9 Standard
Shield
Verificação
Agendador
Quarentena
Relatório
Geral
Antivírus
Atualização
Nome do arquivo
Nome do vírus
Suspeito com
Enviado
A Quarentena não tem um tamanho limite (0 KB).
Mais detalhes
Adicionar
Apagar
Restaurar
Enviar
Opções
Quarentena
A Quarentena armazena arquivos suspeitos para análise. Enquanto estiver na Quarentena, arquios não podem ser executados ou lidos. Você pode escolher não enviar arquivos para análise. Para copiar um arquivo suspeito para a Quarentena, clique no botão "Adicionar" ou arraste e solte o arquivo na lista da Quarentena. Clique 'Recuperar' para mover arquivos para fora da Quarantena, de volta no seu local original.
Mais Ajuda
Quarentena

O BitDefender permite isolar os arquivos infectados ou suspeitos em uma área segura, chamada quarentena. Isolando esses arquivos, o risco de ser infectado desaparece e, ao mesmo tempo, você tem a possibilidade de enviar esses arquivos para futura análise da BitDefender Labs.

O componente que assegura a administração dos arquivos isolados é a **Quarentena**. Esse módulo foi desenvolvido com a função de automaticamente enviar os arquivos infectados para a BitDefender Labs.

Como você pode notar, a seção **Quarentena** contém uma lista de todos os arquivos que foram isolados até o momento. Todo arquivo tem consigo seu nome, tamanho, data de isolamento e data de envio. Se você deseja ver mais informações sobre os arquivos da quarentena clique em **Mais detalhes**.

### Nota

Quando o vírus está na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executado ou lido.

A seção **Quarantine** contém alguns botões para administrar esses arquivos.

- **Adicionar** - adiciona arquivos a quarentena. Use esse botão para isolar um arquivo que você suspeita que tenha sido infectado. Uma janela abrirá e você pode escolher o arquivo de seu local no disco. Dessa forma o arquivo é copiado para a quarentena.

  Se você quer mover o arquivo para a quarentena, deve marcar a caixa **Apagar do local original**. Um modo mais rápido para incluir arquivos suspeitos na quarentena é arrastar e soltar os arquivos na lista da quarentena.

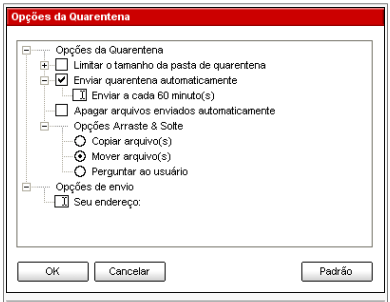
- **Apagar** - apaga os arquivos selecionados de seu computador;

- **Restaurar** - retorna o arquivo selecionado a seu local original.

- **Enviar** - envia os arquivos selecionados para a BitDefender Labs.

**Importante**
Você deve especificar alguma informação antes de enviar estes arquivos. Para isto, clique em **Configurações** e preencha os campos da seção **Opções de e-mail**, como descrito abaixo.

- **Opções** - abre as opções avançadas para a zona de quarentena. A seguinte janela vai aparecer:




Opções da quarentena

As opções de quarentena estão agrupadas em duas categorias:
- **Opções da quarentena**
- **Opções de envio**

**Nota**
Clique na caixa com "+" para abrir uma opção ou na caixa com "-" para fechar uma opção.

Opções de Quarentena

- **Limitar o tamanho da pasta de quarentena** - mantém sobre controle o tamanho da quarentena. Esta opção está habilitada por padrão e o seu tamanho é de 12000 kB. Se você deseja mudar este valor digite um número novo no campo correspondente. Se você selecionar a caixa correspondente a **Apagar arquivos antigos automaticamente**, quando a quarentena estiver cheia e você acrescentar um novo arquivo, os arquivos mais antigos em quarentena serão automaticamente apagados para oferecer espaço livre ao novo arquivo.

- **Enviar quarentena automaticamente** - envia automaticamente os arquivos em quarentena para a BitDefender Labs para futura análise. Você pode ajustar o intervalo de tempo entre dois processos de envios consecutivos em minutos no campo **Enviar quarentena a cada**.

- **Apagar arquivos enviados automaticamente** - apaga automaticamente os arquivos em quarentena após enviá-los para a BitDefender Labs para análise.

- **Opções Arraste & Solte** - se você utilize o método Arrastar e Soltar para incluir arquivos na quarentena, você pode especificar arqui a ação: copiar, mover ou perguntar.

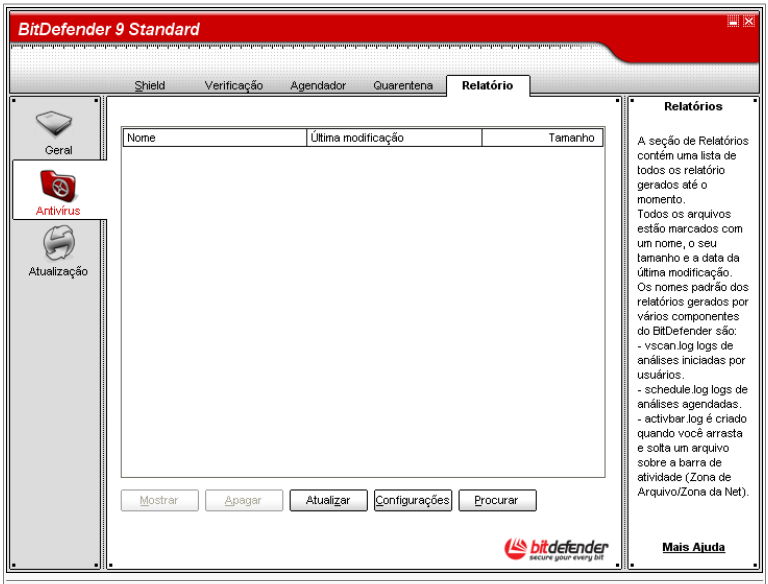
Opções de envio

- **Seu endereço** - digite seu endereço de e-mail caso você queira receber e-mail de nossos especialistas, sobre arquivos suspeitos submetidos para análise.

Clique em **OK** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.

## 7.4. Relatório

Para acessar esta seção clique na aba **Relatório** do módulo de **Antivírus**.


BitDefender 9 Standard
Shield
Verificação
Agendador
Quarentena
Relatório
Geral
Antivírus
Atualização
Nome
Última modificação
Tamanho
Mostrar
Apagar
Atualizar
Configurações
Procurar
Relatórios
A seção de Relatórios contém uma lista de todos os relatório gerados até o momento.
Todos os arquivos estão marcados com um nome, o seu tamanho e a data da última modificação.
Os nomes padrão dos relatórios gerados por vários componentes do BitDefender são:
- vscan.log logs de análises iniciadas por usuários.
- schedule.log logs de análises agendadas.
- activbar.log é criado quando você arrasta e solta um arquivo sobre a barra de atividade (Zona de Arquivo/Zona da Net).
Mais Ajuda

Relatório

A seção **Relatório** contém uma lista de relatórios que foram gerados até agora. Todo arquivo tem incluso seu nome, tamanho e a data da última modificação.

Quando iniciar um processo de verificação, o usuário tem a possibilidade de optar por criar um relatório onde ele pode ver informações sobre o processo de verificação. O usuário pode ver esses relatórios direto do console de gerenciamento.

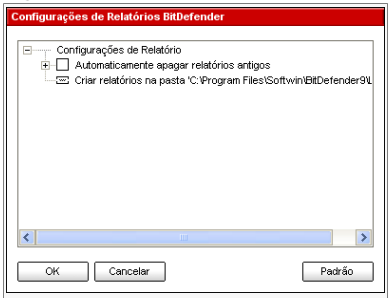
O BitDefender acompanhará sua própria atividade em seu computador. Os relatórios padrão são os seguintes:

- vscan.log é criado quando você executa a verificação de seu sistema;
- schedule.log é das verificações que você agendou;
- activbar.log é criado quando você utiliza o recurso Arrastar & Soltar.

A seção **Relatório** contém alguns botões criados para a administração desses relatórios. A função de cada botão é explicada a seguir:

**Nota**
Os relatórios são salvos por padrão na pasta onde o BitDefender é instalado. Se você salvou os relatórios em outro diretório, você deve usar o botão **Procurar**.

- **Mostrar** - abre o relatório selecionado;
- **Apagar** - apaga o relatório selecionado;
- **Atualizar** - atualiza a seção **Relatório**. Se o console de gerenciamento é aberto na seção **Relatório** e nesse tempo você realizar uma verificação em seu computador, o novo relatório só será exibido quando você clicar em **Atualizar**.
- **Procurar** - abre uma janela em que você pode selecionar os relatórios que deseja ver.
- **Configurações** - abre as opções avançadas para arquivos de relatório. A seguinte janela aparecerá:



Configurações

**Nota**
Clique na caixa com "+" para abrir uma opção ou na caixa com "-" para fechar uma opção.

- **Automaticamente apagar relatórios antigos** - mantém sobre controle o número de arquivos de relatório, apagando aqueles mais velhos que um determinado número de dias. O padrão é 180 dias. Se você deseja mudar este valor digite um número novo no campo correspondente.
- **Criar relatórios na pasta** - especifica a pasta onde os relatórios serão salvos.

Clique em **OK** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.

# 8. Módulo de Atualização

A seção de **Atualização** deste guia do usuário contém os seguintes tópicos:

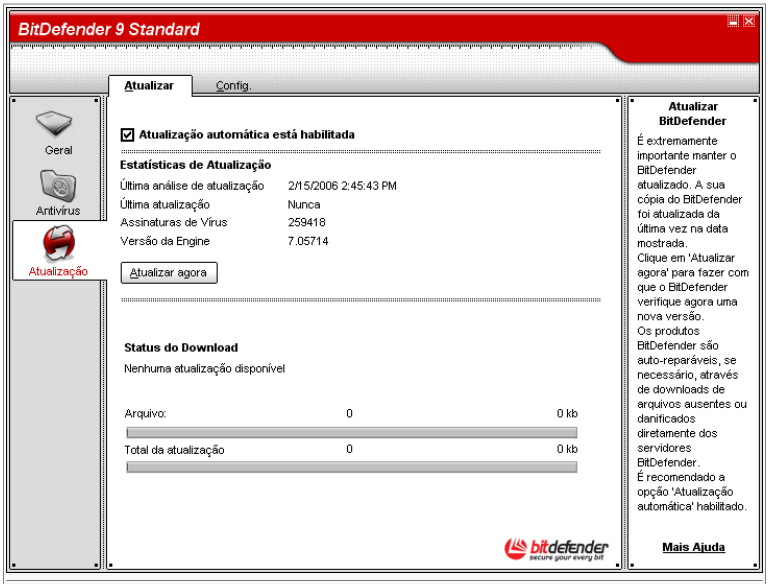
- Atualização automática
- Atualização manual
- Configurações de atualização

**Nota**

Para mais detalher sobre o módulo de **Atualização** verifique a descrição do "*Módulo Atualização*" (p. 33).

## 8.1. Atualização automática

Para acessar esta seção clique na aba **Atualização** do módulo de **Atualização**.


BitDefender 9 Standard
Atualizar
Config.
Geral
Antivírus
Atualização
Atualização automática está habilitada
Estatísticas de Atualização
Última análise de atualização 2/15/2006 2:45:43 PM
Última atualização Nunca
Assinaturas de Vírus 259418
Versão da Engine 7.05714
Atualizar agora
Status do Download
Nenhuma atualização disponível
Arquivo: 0 0 kb
Total da atualização 0 0 kb
Atualizar BitDefender
É extremamente importante manter o BitDefender atualizado. A sua cópia do BitDefender foi atualizada da última vez na data mostrada.
Clique em 'Atualizar agora' para fazer com que o BitDefender verifique agora uma nova versão.
Os produtos BitDefender são auto-reparáveis, se necessário, através de downloads de arquivos ausentes ou danificados diretamente dos servidores BitDefender.
É recomendado a opção 'Atualização automática' habilitado.
Mais Ajuda
Atualização automática

Se você se conectar a Internet através de banda-larga ou DSL, o BitDefender se encarrega da atualização. Ele verifica novas assinaturas de vírus quando você liga o seu computador e toda **hora** depois.

Se uma atualização for detectada, dependendo das opções configuradas na seção Opções de Atualização Automática, você será indagado a confirmar a atualização ou a mesma será feita automaticamente.

A atualização automática também pode ser feita a qualquer hora clicando em **Atualizar Agora**. Também conhecido por **Atualização a pedido do usuário**.

O módulo de **Atualização** irá conectar ao servidor de atualização do BitDefender e verificará se uma atualização está disponível. Caso seja verdadeiro, dependendo das opções configuradas na seção Tipo de Atualização Manual, você será indagado a confirmar a atualização ou a mesma será feita automaticamente.

**Importante**

Talvez seja necessário reiniciar o computador depois da atualização. Caso seja necessário, recomendamos que o faça o mais rápido possível.

**Nota**
Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de atualizar o BitDefender a pedido do usuário.

## 8.2. Atualização Manual

Este método permite instalar as mais novas definições de vírus. Para atualizar a versão use a Atualização automática.

**Importante**
Use a atualização manual quando a automática não puder ser executada ou o computador não estiver conectado a Internet.

Existem 2 modos de atualização manual:

- Com o arquivo `weekly.exe`;
- Com `arquivos zip`.

### 8.2.1. Atualização manual com `weekly.exe`

O pacote de atualização `weekly.exe` é lançado toda sexta-feira e inclui todas as definições de vírus e atualizações do motor de análise disponível até a data.

Para atualizar o BitDefender usando `weekly.exe`, siga os passos a seguir:

1. Faça download do weekly.exe e salve ele localmente no seu disco rígido.
2. Localize o arquivo e clque duplamente nele para executar o assistente de atualização.
3. Clique em **Seguinte**.
4. Marque **Eu aceito os termos do Acordo de Licença** e clique em **Seguinte**.
5. Clique em **Instalar**.
6. Clique em **Concluir**.

### 8.2.2. Atualização manual com `arquivos zip`

Existem 2 arquivos zip no servidor de atualização, contendo atualizações do motor de análise e das assinaturas de vírus: `cumulative.zip` e `daily.zip`.

- `cumulative.zip` é lançado toda segunda-feira e inclui atualizações de definições de vírus e do motor de análise até a data.
- `daily.zip` é lançado a diaramente e inclui atualizações de definições de vírus e do motor de análise desde o último cumulativo até a data atual.

O BitDefender uma arquitetura baseada em serviço. Por isso o procedimento para a atualização das definições de vírus é diferente dependendo do sistema operacional:

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

## Windows NT-SP6, Windows 2000, Windows XP

Passos a seguir:

1. **Fazer o download apropriado .** Se for segunda-feira, faça download do cumulative.zip e salve no disco quando perguntado. Caso contrário faça download do daily.zip e salve no seu disco. Se esta for a primeira atualização manual, faça download dos dois arquivos.
2. Suspenda a proteção antivírus do BitDefender
   - **Saia do console de gerenciamento do BitDefender .** Clique com o botão direito no ícone do BitDefender na Barra de Tarefas e selecione **Sair**.
   - **Abra Serviços .** Clique **Iniciar**, depois **Painel de Controle**, clique duplamente em **Ferramentas administrativas** e clique **Serviços**.
   - **Pare o serviço BitDefender Virus Shield .** Selecione o serviço **BitDefender Virus Shield** na lista e clique em **Parar**.
   - **Pare o serviço BitDefender Scan Server .** Selecione o serviço **BitDefender Scan Server** na lista e clique em **Parar**.
3. **Extrair o conteúdo do arquivo .** Comece com o `cumulative.zip` quando os dois arquivos de atualiuzação estiverem disponíveis. Extraia o conteúdo para a pasta `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` e aceite a substituição dos arquivos.
4. Reinicie a proteção antivírus do BitDefender.

- **Inicie o serviço BitDefender Scan Server .** Selecione o serviço **BitDefender Scan Server** na lista e clique em **Iniciar**.
- **Inicie o serviço BitDefender Virus Shield .** Selecione o serviço **BitDefender Virus Shield** na lista e clique em **Iniciar**.
- Abra o Console de Gerenciamento do BitDefender.

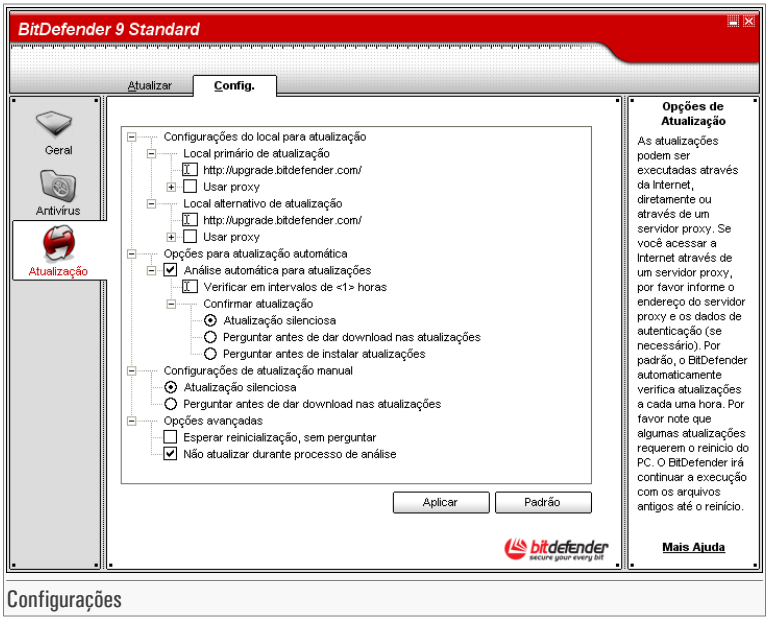
### Windows 98, Windows Millennium

Passos a seguir:

1. **Fazer o download apropriado .** Se for segunda-feira, faça download do cumulative.zip e salve no disco quando perguntado. Caso contrário faça download do daily.zip e salve no seu disco. Se esta for a primeira atualização manual, faça download dos dois arquivos.
2. **Extrair o conteúdo do arquivo .** Comece com o `cumulative.zip` quando os dois arquivos de atualiuzação estiverem disponíveis. Extraia o conteúdo para a pasta `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` e aceite a substituição dos arquivos.
3. Reinicie o computador.

## 8.3. Configurações

Para acessar esta seção clique na aba **Configurações** do módulo de **Atualização**.


BitDefender 9 Standard
Atualizar
Config.
Geral
Antivírus
Atualização
Configurações do local para atualização
Local primário de atualização
http://upgrade.bitdefender.com/
Usar proxy
Local alternativo de atualização
http://upgrade.bitdefender.com/
Usar proxy
Opções para atualização automática
Análise automática para atualizações
Verificar em intervalos de <1> horas
Confirmar atualização
Atualização silenciosa
Perguntar antes de dar download nas atualizações
Perguntar antes de instalar atualizações
Configurações de atualização manual
Atualização silenciosa
Perguntar antes de dar download nas atualizações
Opções avançadas
Esperar reinicialização, sem perguntar
Não atualizar durante processo de análise
Aplicar
Padrão
Opções de Atualização
As atualizações podem ser executadas através da Internet, diretamente ou através de um servidor proxy. Se você acessar a Internet através de um servidor proxy, por favor informe o endereço do servidor proxy e os dados de autenticação (se necessário). Por padrão, o BitDefender automaticamente verifica atualizações a cada uma hora. Por favor note que algumas atualizações requerem o reinício do PC. O BitDefender irá continuar a execução com os arquivos antigos até o reinício.
Mais Ajuda
Configurações

Atualizações podem ser feitas da rede local, pela Internet, diretamente ou por um servidor Proxy.

A janela com as opções de atualização contém 4 categorias de opções (**Configurações do local para atualização**, **Opções para atualização automática**, **Configurações de atualização manual** e **Opções avançadas**) organizadas em um menu expansível, similar aos do Windows.

**Nota**

Clique na caixa com "+" para abrir uma opção ou clique na caixa com "-" para fechar uma opção.

## 8.3.1. Configurações do local para atualização

Para atualizações melhores e mais rápidas, você pode configurar dois locais de atualização: uma **Local de atualização primário** e uma **Local de atualização alternativo**. Para ambos você deve configurar as seguintes opções:

- **Local de Atualização** - Se você estiver conectado a uma rede local que tem um arquivo de assinaturas de vírus BitDefender localmente, você pode mudar o local de atualização aqui. Por padrão ele é: http://upgrade.bitdefender.com.
- **Usar Proxy** - Caso uma empresa use um servidor Proxy marque essa opção. As opções seguintes devem ser especificadas:
  - **Configurações do proxy** - digite o IP ou o nome do servidor Proxy e a porta que o BitDefender usa para se conectar ao servidor Proxy.

    Importante
    Sintaxe: `nome:porta` ou `ip:porta`.

  - **Usuário do proxy** - digite um usuário reconhecido pelo Proxy.

    Importante
    Sintaxe: `domínio\usuário`.

  - **Senha do proxy** - digite a senha válida para o usuário especificado anteriormente.

## 8.3.2. Opções para atualização automática

- **Análise para atualização automática** - assegura que o BitDefender procure atualizações em nossos servidores.
- **Verificar em intervalos de x horas** - Define de quanto em quanto tempo o BitDefender procura atualizações. O intervalo padrão é 1 hora.
- **Atualização Silenciosa** - O BitDefender faz download automaticamente e implementa a atualização.
- **Perguntar antes de dar download nas atualizações** - todas as vezes que uma atualização estiver disponível, você será indagado antes do download ser feito.
- **Perguntar antes de instalar atualizações** - todas as vezes que uma atualização for feita em download, você será perguntado antes de instalá-la.

**Importante**
Se você selecionar **Perguntar antes de dar download nas atualizações** ou **Perguntar antes de instalar atualizações** e você selecionar fechar&sair a console de gerenciamento a atualização automática não se realizará.

## 8.3.3. Configurações de atualização manual

- **Atualização silenciosa** - a atualização manual pode será automaticamente sem intervenção.
- **Perguntar antes de dar download nas atualizações** - toda vez que você executa uma atualização manual será perguntado antes de baixar e instalar as atualizações.

**Importante**
Se você selecionar **Perguntar antes de dar download nas atualizações** e você fechar&sair da console de gerenciamento, a atualização manual não será executada.

## 8.3.4. Opções avançadas

- **Esperar reinicialização, sem perguntar** - Se uma atualização requerer uma inicialização, o produto continuará funcionando com os arquivos antigos até o sistema reiniciar. O usuário não será indagado para reiniciar o sistema, sendo assim o processo de atualização do BitDefender não irá interferir no trabalho do usuário.
- **Não atualizar durante processo de análise** - BitDefender não irá atualizar se o rastreamento estiver em andamento. Assim a atualização BitDefender não interfirirá no rastreamento.

**Nota**
Se BitDefender for atualizado durante rastreamento, o rastreamento será abortado.

Clique em **Aplicar** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.

# Melhores práticas

# 9. Melhores práticas

A seção **Melhores práticas** deste manual do usuário contém o tópico:

- Antivírus

## 9.1. Antivírus

Passos a serem seguidos para estar livre de vírus e spyware:

1. Depois de concluído o processo de instalação, registre seu produto, como descrito na seção "*Registro do Produto*" (p. 43).
2. Execute uma atualização a pedido do usuário das assinaturas de vírus e spyware, como descrito na seção "*Atualização automática*" (p. 87).
3. Execute uma análise completa no sistema, como descrito em na seção " *Verificação imediata* " (p. 59).
4. Na seção Status do módulo **Geral**, mantenha habilitado as proteções do BitDefender: **Virus Shield** e **Atualização automática**.
5. Programe seu BitDefender para analisar seu sistema pelo menos uma vez por semana como descrito na seção "*Verificação agendada*" (p. 69).

# CD de Resgate BitDefender

O **BitDefender 9 Standard** vem com um CD executável (CD de Resgate BitDefender baseado no LinuxDefender) capaz de verificar e desinfectar todos os discos fixos antes do seu sistema operacional ser carregado.

Você deve usar o CD de Resgate BitDefender a qualquer momento que o seu sistema operacional não estiver funcionando corretamente por infecção de vírus. Isto normalmente acontece quando você não usa um produto antivírus.

A atualização das assinaturas de vírus é feita automaticamente, sem a intervenção do usuário quando você executa o CD de Resgate BitDefender.

# 10. Resumo

O LinuxDefender é uma distribuição Knoppix re-masterizada pelo BitDefender, que integra a mais nova solução de segurança BitDefender para Linux com o GNU/Linux Knoppix Live CD, oferecendo proteção antivírus/anti-spam para SMTP e um antivírus de estação capaz de verificar e desinfectar os discos fixos existentes (incluindo partições NTFS Windows), compartilhamentos remotos Samba/Windows ou volumes NFS. Uma interface web de configuração das soluções BitDefender também é incluída.

Características

- Proteção instantânea de e-mail (Antivírus & Anti-Spam)
- Soluções antivírus para o seu disco fixo
- Suporte a gravação NTFS (usando Captive project)
- Desinfecção de arquivos infectados em partições Windows XP

## 10.1. O que é KNOPPIX?

Citação de http://knopper.net/knoppix:

“ KNOPPIX é um CD executável com uma coleção de software GNU/Linux (http://www.linux.com/), detecção automática de hardware e suporte para várias placas de vídeo, áudio, SCSI e USB e outros periféricos. KNOPPIX pode ser usado como uma avaliação do Linux, um CD educacional, sistema de resgate, ou adaptado e usado como plataforma para softwares comerciais de avaliação. Não é necessária nenhuma instalação no disco fixo. ”

## 10.2. Requisitos Mínimos

Antes de executar o LinuxDefender você deve primeiramente verificar se seu sistema atende os seguintes requisitos.

**Processador** — Compatível com x86, mínimo de 166 MHz. Um processador de geração i686, de 800MHz, seria uma melhor escolha mínima.

| | |
|---|---|
| **Memória** | O valor mínimo aceitável é de 64MB, o recomendado é de 128MB, para uma melhor performance. |
| **CD-ROM** | LinuxDefender é executado diretamente de um leitor CD-ROM. |
| **Conexão a Internet** | Apesar de o LinuxDefender ser executado sem conexão com Internet, os processos de atualização requerem uma conexão http ativa. Portanto, para uma proteção atualizada, a conexão com a Internet é prioritária. |
| **Resolução gráfica** | Uma resolução gráfica de 800x600 é recomendada para administração via web. |

## 10.3. Software incluído

O CD de Resgate BitDefender inclui os seguintes pacotes de programas.

- BitDefender SMTP Proxy (Anti-Spam & Antivírus)
- BitDefender Remote Admin (configuração via web)
- BitDefender Linux Edition (verificador antivírus) + Interface GTK
- Documentação BitDefender (formatos PDF & HTML)
- BitDefender Extras
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Ferramentas para recuperação de dados e de reparo do sistema, mesmo para sistemas operacionais
- Ferramentas de análise de rede e segurança para administradores de redes
- Solução de backup Amanda
- thttpd
- Analisador de tráfego de rede Ethereal, IPTraf IP LAN Monitor
- Auditor de segurança de rede Nessus
- Solução de reparo de reconstrução de partições Parted, QTParted e partimage
- Adobe Acrobat Reader
- Mozilla Firefox Web browser

# 10.4. Soluções BitDefender para Linux

O LinuxDefender CD inclui o BitDefender SMTP Proxy Antivirus/Antispam for Linux, o BitDefender Remote Admin (uma interface web para configurar o BitDefender SMTP Proxy) e o verificador antivírus por demanda BitDefender Linux Edition.

## 10.4.1. BitDefender SMTP Proxy

O BitDefender for Linux Mail Servers - SMTP Proxy é uma solução inspetora de conteúdo seguro, o qual providencia proteção antivírus e anti-spam em nível de gateway, verificando todo tráfego de e-mail para malware conhecidos e desconhecidos. Como resultado de uma tecnologia proprietária única, o BitDefender for Mail Servers é compatível com a maioria das plataformas de e-mail e certificadas como "RedHat Ready".

Esta solução de Antivírus e Anti-Spam verifica, desinfecta e filtra o tráfego de e-mail para qualquer servidor de e-mail existente, não importando a plataforma ou sistema operacional. O BitDefender SMTP Proxy é executado em boot e verifica todo tráfego de chegada de e-mail. Para configurar o BitDefender SMTP Proxy, use o BitDefender Remote Admin, usando as instruções abaixo.

## 10.4.2. BitDefender Remote Admin

Você pode configurar e gerenciar os serviços BitDefender remotamente (depois de ter configurado sua rede) ou localmente, seguindo estes passos:

1. Execute o navegador Firefox carregue a URL do BitDefender Remote Admin: https://localhost:8139 (ou clique duplamente no ícone do BitDefender Remote Admin no seu desktop)
2. Digite o usuário "bd" e a senha "bd"
3. Escolha "SMTP Proxy" no menu esquerdo
4. Configure o servidor SMTP real e a porta de escuta
5. Adicione domínios de e-mails para relay
6. Adicione domínios de rede para relay
7. Escolha "AntiSpam" no menu esquerdo para configurar as capacidades anti-spam
8. Escoha "AntiVirus" para configurar as ações do Antivírus BitDefender (o que e quando fazer quando um vírus for encontrado, local da quarentena)
9. Adicionalmente, você pode configurar as notificações "Mail notifications" e as funções de log ("Logger")

### 10.4.3. BitDefender Linux Edition

O verificador antivírus incluído no LinuxDefender e integrado diretamente no desktop. Esta versão oferece uma interface gráfica GTK+.

Apenas navegue no seu disco fixo (ou compartilhamentos remotos), clique com o botão direito em qualquer arquivo ou pasta e selecione "Scan with BitDefender". O BitDefender Linux Edition irá verificar os itens selecionados e mostrará um relatório de status. Para mais opções leia a documentação do BitDefender Linux Edition (na pasta de documentação BitDefender ou página manual) e o programa **/opt/BitDefender/lib/bdc**.

# 11. Guia LinuxDefender

## 11.1. Iniciar e parar

### 11.1.1. Iniciar LinuxDefender

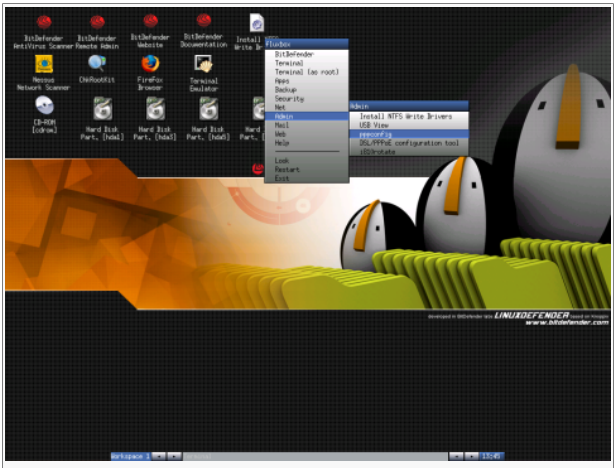
Para iniciar o CD, configure a BIOS do seu computador para iniciar diretamente do CD, coloque o CD no drive e reinicie o computador. Tenha certeza que o seu computador pode iniciar do CD.

Espere até a próxima tela aparecer e siga as instruções na tela para iniciar o LinuxDefender.

Tela de inicialização

Pressione F2 para opções detalhadas. Pressione F5 para opções detalhadas em Espanhol. Parar uma inicialização rápida com as opções padrões, apenas pressione ENTER.

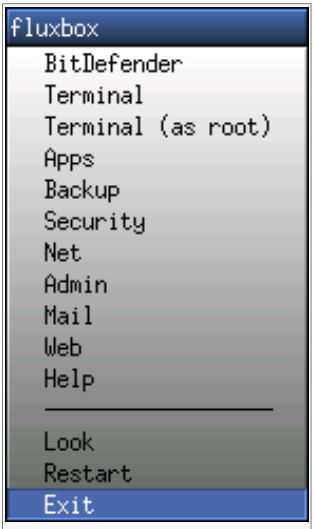
Quando o processo finalizar você verá o próximo desktop. Você pode agora usar o LinuxDefender.



O Desktop

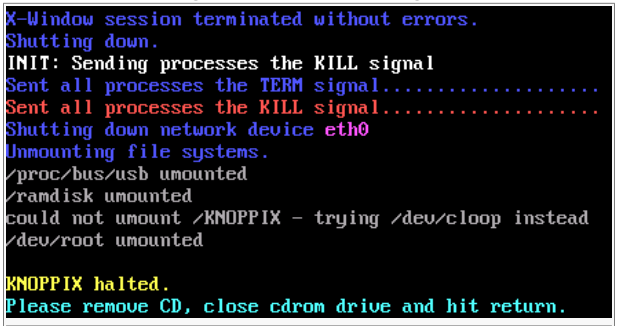
## 11.1.2. Parar LinuxDefender

Para sair de maneira apropriada do LinuxDefender é recomendado desmontar todas as partições montadas usando o comando **umount** ou clicando com o botão direitonos icons da partição no desktop e selecione **Unmount**. Então você pode seguramente desligar o seu computador selecionando **Exit** do menu LinuxDefender (clique com o botão direito para abrir) ou digitando o comando **halt** em um terminal.




Escolha "EXIT"

Quando o LinuxDefender fechar com sucesso todos os programas ele irá mostrar uma tela como a imagem seguinte. Você pode remover o CD para iniciar através do seu disco local. Agora você pode desligar o seu computador ou reiniciá-lo.


X-Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Sent all processes the TERM signal.....
Sent all processes the KILL signal.....
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb umounted
/ramdisk umounted
could not umount /KNOPPIX - trying /dev/cloop instead
/dev/root umounted
KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.

Espere por esta mensagem enquanto desligando

## 11.2. Configure a conexão de Internet

Se você estiver em uma rede DHCP e você tiver uma placa de rede ethernet, uma conexão de Internet já deveria estar detectada e configurada. Para uma configuração manual, siga os próximos passos.

1. Abra o menu LinuxDefender (clique direito) e selecione **Terminal** parar abrir o console.
2. Digite **netcardconfig** no terminal aberto para executar a ferramenta de configuração de rede.
3. Se sua rede estiver usando DHCP, selecione **yes** (se você não tiver certeza, pergunte ao seu administrador da rede). Senão, verifique abaixo.
4. A conexão de rede deveria estar autmaticamente configurada agora. Você pod ever seu IP e as configurações da placa de rede com o comando **ifconfig**.
5. Se você tiver um IP estático (não estiver usando DHCP), escolha **No** na pergunta sobre o DHCP.
6. Siga as instruções. Se você não tiver certeza do que está fazendo, contacte o administrador da rede para detalhes.

Se tudo correu bem, você pode testar a conexão usando o comando ping para conectar a `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Se você estiver usando uma conexão discada, escolha **pppconfig** do menu LinuxDefender /Admin. Depois siga as instruções na tela para configurar uma conexão PPP com a Internet.

## 11.3. Atualização BitDefender

Os pacotes BitDefender para o LinuxDefender usam arquivos atualizáveis. Desta forma, você pode atualizar todas as assinaturas de vírus, mecanismos de verificação ou base de dados do anti-spam, mesmo que você esteja executando o sistema de uma mídia de leitura apenas, como o LinuxDefender CD.

Tenha certeza que você tenha uma conexão com a Internet ativa. Primeiramente abra o BitDefender Remote Admin e selecione **Live! Update** do menu esquerdo. Pressione **Update Now** para checar novas atualizações.

Alternativamente, você pode digitar o seguinte comando no terminal.

```
# /opt/BitDefender/bin/bd  update
```

Todos os processos de atualizações são registrados no BitDefender log. Você pode vê-lo com o seguinte comando.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Se você estiver usando uma proxy para conexões, configure as configurações de Proxy no menu **Live! Update**, na aba **Configuration**.

# 11.4. Verificação de Vírus

## 11.4.1. Como acessar os dados do Windows?

### Suporte a Escrita NTFS

Suporte a escrita NTFS está disponível usando Captive NTFS write project. Você precisa de dois arquivos da instalação do Windows: `ntoskrnl.exe` e `ntfs.sys`. No momento, apenas dispositivos do Windows XP têm suporte. Note que você também pode usá-los para acessar partições Windows 2000/NT/2003.

### Instalando os dispositivos NTFS

Para acessar as partições Windows NTFS e para poder escrever dados nestas partições, você terá que instalar os dispositivos NTFS primeiramente. Se você não estiver usando NTFS para suas partições Windows, mas FAT, você vai precisar de acesso de leitura apenas para os seus dados, você pode montar diretamente os discos e acessar o Windows como se fosse um disco Linux.

Para adicionar suporte para partições NTFS, você deve instalar os dispositivos NTFS, do seu disco fixo, compartilhamentos remotos, memória USB ou do Windows Update. É recomendado usar os dispositivos de um lugar seguro, pois os dispositivos locais do Windows podem conter vírus ou estar corrompidos.

Clique duplamente no ícone **Install NTFS Write Drivers** para executar o **BitDefender Captive NTFS Installer**. Selecione a primeira opção se você quiser instalar os dispositivos do disco local.

Se os dispositivos estiverem no mesmo lugar, use o **Quick search** para encontrar os dispositivos.

Alternativamente, você pode especificar onde os dispositivos devem ser encontrados. Ou você pode baixar os dispositivos do Windows Update SP1.

Os dispositivos não serão instalados no disco fixo, mas temporariamente usados pelo LinuxDefender para acessar partições Windows NTFS. Se o programa instalar os dispositivos NTFS, você pode clicar duplamente nos ícones das partições NTFS e explorar o conteúdo. Para um melhor gerenciamento de arquivos, use o Midnight Commander do menu LinuxDefender (ou digite **mc** na console).

### 11.4.2. Como executo uma verificação antivírus?

Navegue pelas pastas, clique com o botão direito em um arquivo ou pasta e selecione **Enviar**. Então escolha **BitDefender Scanner**.

Ou você pode digitar o próximo comando no terminal. O **BitDefender Antivirus Scanner** irá começar pelo arquivo ou pasta selecionada como local padrão de verificação.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Depois clique em **Start Scan**.

Se você quer configurar as opções antivírus, selecione a aba **Configure Antivirus** no lado esquerdo do programa.

## 11.5. Construindo um filtro instantâneo de e-mail

Você pode usar o LinuxDefender para criar uma solução de filtro instantânea de e-mail, sem instalar qualquer software ou modificar o servidor de e-mail. A idéia é colocar o LinuxDefender na frente do seu servidor de e-mail, permitindo ao BitDefender verificar todo o tráfego SMTP contra spam e vírus e redirecioná-lo para o seu servidor de e-mail real.

### 11.5.1. Pré-requisitos

Você precisará de um PC com uma CPU compatível com Pentium 3 ou maior, pelo menos 256MB de RAM e um drive CD/DVD. O sistema LinuxDefender irá receber o

tráfego SMTP ao invés do servidor real de e-mail. Existem várias maneiras de configurar isto.

1. Troque o IP do seu servidor de e-mail real e aponte o velho IP para p sistema LinuxDefender
2. Troque seu DNS para que a entrada do MX para todos os domínios esteja apontada para o sistema LinuxDefender
3. Configure os seus clientes de e-mail para usar o novo sistema LinuxDefender como servidor SMTP
4. Modifique sua configuração do firewall para encaminhar / redirecionar todas as conexões SMTP para o sistema LinuxDefender ao invés do servidor real de e-mail

Para mais informações você deve consultar. For more information you may consult Linux Networking guides e Netfilter documentation.

## 11.5.2. O Filtro de e-mail

Inicie o seu LinuxDefender CD e espere até que o sistema X Windows esteja carregado e funcional.

Para configurar o BitDefender SMTP Proxy, clique duplamente no ícone **BitDefender Remote Admin** no desktop. A seguinte janela aparecerá. Use o nome de usuário `bd` e senha `bd` para entrar no BitDefender Remote Admin.

Depois de uma autenticação de sucesso, você poderá configurar o BitDefender SMTP Proxy.

Escolha **SMTP Proxy** para configurar o servidor de e-mail real que você deseja proteger contra vírus e spam.

Selecione a aba **Email domains** para digitar todos os domínios que você deseja aceitar e-mails.

Pressione **Add Email Domain** ou **Add Bulk Domains** e siga as instruções na tela para configurar os domínios de relay de email.

Selecione a aba **Net domains** para digitar todas as redes que você deseja redirecionar e-mails.

Pressione **Add Net Domain** ou **Add Bulk Net Domains** e siga as instruções para configurar os domínios para redirecionar.

Selecione **Antivirus** do menu esquerdo para escolher o que fazer quando um vírus for encontrado e para configurar outras opções de antivírus.

Agora, todo tráfego SMTP é verificado e filtrado pelo BitDefender. Por padrão, todas as mensagens com vírus são limpas ou descartadas e todas as mensagens spam detectadas pelo BitDefender serão marcadas com a palavra `[SPAM]` no campo Assunto. Um cabeçalho de e-mail (`X-BitDefender-Spam: Yes/No`) é adicionado a todos os e-mails para facilitar o filtro do cliente.

## 11.6. Exexutar auditoria de segurança de rede

Além da capacidade anti-malware, recuperação de dados e filtragem de e-mails, LinuxDefender vem com uma série de ferramentas para executar uma auditoria completa de segurança de rede. Análise forense em sistemas comprometidos também é possível usando as ferramentas de segurança incluídas no LinuxDefender. Leia este pequeno guia e aprenda como você pode uma rápida e segura auditoria nos servidores ou redes.

### 11.6.1. Verificar rootkits

Antes de procurar por problemas de segurança, primeiramente deve-se ter certeza que o computador com o LinuxDefender não está comprometido. Você pode executar uma verificação de vírus em discos fixos instalados, como mostrado no guia **Scan for viruses** ou você pode procurar por Unix rootkits.

Primeiro monte todas as partições do disco clicando duplamente no ícone do desktop ou usando o comando **mount** na console. Depois clique duplamente no ícone **ChkRootKit** para checar o conteúdo do CD ou executar o comando **chkrootkit** da console, usando o parâmetro `-r NEWROOT` para especificar o novo diretório / (root) do host.

```
# chkrootkit -r /dev/hda3
```

Seu um rootkit for encontrado, chkrootkit irá mostrá-lo em **NEGRITO**, usando letras maiúsculas.

### 11.6.2. Nessus – O Verificador de Rede

**O que é Nessus.** “ Nessus é o mais popular analisador de vulnerabilidades open-source usado em mais de 75,000 empresas no mundo. Muitas das maiores organizações estão reduzindo significantemente seus custos usando Nessus como auditor e dispositivos e aplicativos. ”

O Nessus pode ser usado remotamente para verificar várias vulnerabilidades nos computadores de rede. Ele também recomenda ações a serem tomadas para diminuir riscos de segurança e prevenir incidentes.

Clique duplamente no ícone **Nessus Security Scanner** ou execute **startnessus** de um terminal. Espere até a próxima janela aparecer. Dependendo dos recursos do hardware, pode levar até 10 minutos para carregar o Nessus, junto com a sua base de dados de mais de 5000 vulnerabilidades. Use o usuário `knoppix` e a senha `knoppix` para acessar.

Clique na aba **Target selection** e digite o IP do computador IP ou nome de computadores que você quer verificar por vulnerabilidades. Tenha certeza em customizar todas as opções de verificação de acordo com a configuração do seu sistema para evitar sobrecarga de tráfego de rede. Depois clique em **Start the scan**.

Quando o processo de verificação estiver complete, Nessus mostrará os resultados e as recomendações. Você pode salvar o relatório em vários formatos, incluindo HTML com gráficos.

## 11.7. Verifique a RAM do seu sistema

Normalmente, quando seu sistema tem um comportamento anormal (paralisa ou reinicializa sozinho de tempos em tempos), pode ser um problema de memória. Você pode testar os módulos RAM com o programa **memtest**, descrito abaixo.

Inicie seu computador a partir do LinuxDefender CD. Digite **memtest** na hora da inicialização e pressione Enter.

O programa Memtest executará vários testes para checar a situação da memória RAM. Você pode configurar que testes executar ou outras opções pressionando `c`.

Um Memtest complete pode levar até 8 horas, dependendo da capacidade e velocidade RAM do seu sistema. É recomendado deixar o Memtest executar todos os testes para verificar os erros de RAM. Você pode sair a qualquer momento, pressionando `ESC`.

Se você pretende comprar um novo hardware é recomendado usar o LinuxDefender e o memtest para verificar erros ou problemas de compatibilidade.

# Ajuda

# 12. Suporte

## 12.1. Departamento de suporte

Como um fabricante de valor agregado, a SOFTWIN garante um nível de serviço sem precedentes de suporte rápido e qualificado. O centro de suporte listado abaixo é continuamente atualizado com as mais novas descrições de vírus e respostas para perguntas comuns, para que você possa obter a informação necessária de uma forma rápida.

Na SOFTWIN, dedicação para economizar dinheiro e tempo dos clientes providenciando os produtos mais avançados em preço competitivos sempre foi a principal prioridade. Além disso, consideramos que um negócio de sucesso é baseado em boa comunicação e comprometimento em suporte ao cliente.

Encorajamos você a pedir ajuda ao suporte em <support@bitdefender.com> a qualquer hora. Para uma resposta rápida, por favor inclua no seu e-mail o máximo de detalhes sobre seu produto, sistema e a descrição do problema.

## 12.2. Ajuda on-line

### 12.2.1. BitDefender Knowledge Base

O BitDefender Knowledge Base é um repositório on-line de informação sobre os produtos BitDefender. Ele armazena em formato facilitado relatórios sobre resultados de problemas técnicos e questionamentos sendo analisados pela equipe de suporte e desenvolvimento BitDefender, com artigos de informações gerais sobre prevenção de vírus, gerenciamento das soluções e explicações detalhadas.

O BitDefender Knowledge Base é aberto ao público e gratuito. Este rico meio de informação é outra forma de providenciar aos clientes BitDefender conhecimento técnico e visão necessária. Todas as requisições sobre problemas encontrados por clientes BitDefender eventualmente acabam chagando ao BitDefender Knowledge Base, como relatórios de bugfix e arquivos de ajuda.

O BitDefender Knowledge Base está disponível em http://kb.bitdefender.com.

# 12.3. Informação sobre contato

Comunicação eficiente é a chave para um negócio de sucesso. Nos últimos 10 anos a SOFTWIN estabeleceu uma reputação indiscutível excedendo as expectativas dos clientes e parceiros, sempre buscando uma melhor comunicação. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.

## 12.3.1. Endereços Web

Departamento de Vendas: <sales@bitdefender.com>
Suporte Técnico: <support@bitdefender.com>
Documentação: <documentation@bitdefender.com>
Programa de Parcerias: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Relações Públicas: <pr@bitdefender.com>
Oportunidades de Emprego: <jobs@bitdefender.com>
Envio de Vírus: <virus_submission@bitdefender.com>
Envio de Spam: <spam_submission@bitdefender.com>
Relato de Abuso: <abuse@bitdefender.com>
Página Web de Produtos: http://www.bitdefender.com
Arquivos de Produtos FTP: ftp://ftp.bitdefender.com/pub
Distribuidores Locais: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

## 12.3.2. Endereço

Os escritórios BitDefender estão prontos a responder quaisquer dúvidas na respectiva área de operação, comercialmente e assuntos gerais. Seus endereços respectivos estão listados abaixo.

### Alemanha

**Softwin GmbH**
Karlsdorfer Straße 56 88069
Tettnang
Technischer Support: <support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Product web site: http://www.bitdefender.de

## Espanha

**Constelación Negocial, S.L**
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

## E.U.A

**BitDefender LLC**
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support: <support@bitdefender.us>
Sales: <sales@bitdefender.us>
Phone: 954 776 62 62, 800 388 80 62
Fax: 954 776 64 62, 800 388 80 64
Product web site: http://www.bitdefender.us

## Romania

**SOFTWIN**
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

# 13. Perguntas Mais Freqüentes

## 1. Geral

P: Como posso saber se o BitDefender está mesmo funcionando?

R: No módulo **Geral**, acesse a seção Status e veja as estatísticas.

P: Quais são os requisitos do sistema?

R: Você poderá achá-los na seção "*Requisitos Mínimos*" (p. 19).

P: Como eu desinstalo o BitDefender?

R: O procedimento de remoçào é descrito na seção "*Remoção, reparo ou modificação das funções do BitDefender*" (p. 22).

P: Como posso registrar o BitDefender?

R: O processo de registro está descrito na seção "*Registro do Produto*" (p. 43).

## 2. Antivírus

P: Como posso realizar uma verificação completa do sistema?

R: No módulo **Antivírus**, acesse a seção Verificação, marque **Unidades Locais** e clique em **Verificar**.

P: Quando devo verificar meu computador?

R: Recomendamos que você verifique o sistema pelo menos uma vez por semana.

P: Como posso verificar automaticamente todos os arquivos que transferir para meu computador?

R: O BitDefender verifica todos os arquivos no-acesso. Só o que você precisa fazer é manter o Virus Shield ativado.

P: Como posso programar o BitDefender para verificar meu computador periodicamente?

R: No módulo **Antivírus**, acesse a seção Agendador, clique em **Novo** e siga o assistente.

P: O que acontece com os arquivos da zona de quarentena?

R: Você pode enviar esses arquivos para a BitDefender Labs para serem analisados, mas primeiro você deve especificar as configurações de e-mail (acesse a seção Quarentena e clique em **Opções**).

## 3. Atualização

P: Por que é necessário atualizar o BitDefender?

R: Todas as vezes que você executar uma nova atualização de assinatura de vírus será adicionada ao mecanismo de verificação e novas asssinaturas de anti-spyware serão adicionadas a base de dados.

P: Como eu posso atualizar o BitDefender?

R: Por padrão, o BitDefender se atualizará automaticamente a cada hora. Mas você pode mudar o intervalo de tempo para a atualização automática no módulo Atualização.

# Vocabulário

| | |
|---|---|
| Active X | ActiveX é um modelo para escrever programas para que outros programas e seus sistemas operacionais possam buscá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para fazer páginas da Web interativas que se parecem e se comportam como programas de computador, melhor que páginas estáticas. Com o ActiveX, usuários podem perguntar ou responder questões, apertar botões e interagir de outras formas com a página. Controles ActiveX são também escritos usando Visual Basic.<br><br>O ActiveX é notável para uma completa falta de controles de segurança; especialistas em segurança de computador desencorajam seu uso pela Internet. |
| Adware | O Adware é sempre combinado com um programa host sem custo enquanto o usuário concordar em aceitar o adware. Não existem implicações neste tipo de instalação, pois o usuário concordou com o propósito do aplicativo.<br><br>No entanto, propagandas do tipo “pop-up” podem se tornar uma inconveniência, e em alguns casos afetar a performance do seu sistema. Além disto, a informação que alguns destes programas coleta pode causar problemas de privacidade para usuários que não estão totalmente cientes do funcionamento do programa. |
| Arquivo | Um disco, fita ou diretório que contém arquivos que podem ter sido gravados como backup.<br><br>Um arquivo que contém um ou mais arquivos em formato compactado.<br><br>Um documento ou um componente ou parte de um programa. |
| Arquivo de relatório | Um arquivo que lista as ações que ocorreram. Por exemplo BitDefender mantém um arquivo de relatório |

| | |
|---|---|
| | com uma lista dos caminhos verificados, as pastas, o número de arquivos e arquivos compactados verificados, quantos arquivos infectados e suspeitos foram encontrados. |
| Atualização | Uma nova versão do programa ou driver do produto projetado para substituir uma versão antiga do mesmo produto. Além disso, as rotinas de instalação verificam se uma versão mais antiga está instalada no seu computador, caso contrário, você não pode instalar.<br><br>O BitDefender possui um módulo de atualização que permita a você verificar manualmente por atualizações ou deixa que ele automaticamente atualize o produto. |
| Área de notificação | Introduzido com o Windows 95, a área de notificação é localizada na barra de tarefas do Windows (geralmente na parte inferior próxima ao relógio) e contém miniaturas de ícones para fácil acesso de funções do sistema como fax, modem, volume, e outros. Dois cliques ou um clique como o botão direito do mouse para ver ou acessar detalhes dos controles. |
| Backdoor | Um furo na segurança do sistema deixado deliberadamente pelos desenvolvedores os mantenedores. A motivação para tais furos não pe sempre sinistra, alguns sistemas operacionais, por exemplo, saem com contas privilegiadas para uso em campo para serviço dos técnicos ou programa de manutenção dos programadores do fabricante. |
| Caminho | As direções exatas de um arquivo em um computador. Estas direções são descritos geralmente por meio do sistema de arquivamento hierárquico de cima para baixo.<br><br>A rota entre dois pontos quaisquer, com os canais de comunicação entre dois computadores. |
| Cliente de e-mail | É uma aplicação que permite a você enviar e receber e-mails. |
| Cookie | Dentro da indústria da Internet, os cookies são descritos como pequenos arquivos de texto que contém informações sobre computadores individuais que podem ser analisados e usados pelos anunciantes para rastrear |

| | |
|---|---|
| | gostos e interesses on-line. Nesse reino, a tecnologia de cookies está sendo desenvolvida ainda e a intenção é direcionar os anúncios diretamente aos seus interesses. É uma espada de dois gumes para muitos porque por um lado é eficiente e pertinente porque só vê anúncios que interessam a você. E por outro lado, envolve "rastrear" e "seguir" a onde você vai e onde está clicando. Compreensível assim, existe um debate sobre a privacidade e muitas pessoas que se sentem ofendidas pelo fato de serem observados com um número SKU (você sabe, o código de barras na parte traseira dos pacotes que são lidos na saída do supermercado). Embora esse ponto de vista possa ser extremo, em alguns casos é exato. |
| Definições de vírus | É um padrão binário de vírus, utilizado pelo programa antivírus para detectar e eliminar os vírus. |
| Download | Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um periférico. O termo é muitas vezes usado para descrever o processo de copiar um arquivo de um serviço on-line para seu próprio computador. Download também pode se referir a copiar um arquivo de um servidor de rede para um computador na rede. |
| E-mail | Correio eletrônico. Um serviço que envia mensagens para computadores em redes locais ou mundiais. |
| Eventos | Uma ação ou ocorrência detectada por um programa. Eventos podem ser ações de usuários, tais como clicar com botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como sem memória. |
| Extensão do arquivo | É a parte do arquivo, após o ponto final, indica o tipo de dados que estão armazenados no arquivo.<br><br>Muitos sistemas operacionais usam extensões de arquivos, ex. Unix, VMS, MS-DOS. Eles são usualmente de uma a três letras e / ou números (alguns sistemas operacionais antigos não suportam mais que três). Exemplos: "c" para códigos em C, "ps" para PostScript, "txt" para texto. |

| | |
|---|---|
| Falso positivo | Ocorre quando a verificação identifica um arquivo infectado quando de fato não está. |
| Heurística | Um método baseado em regras para identificar novos vírus. Esse método de verificação não se baseia em definições de vírus específicas. A vantagem da verificação heurística é que ela não é enganada por uma nova variante do vírus. Entretanto. Entretanto ela pode relatar um código suspeito em um programa normal, gerando assim um chamado "falso positivo". |
| IP | Um protocolo roteável no conjunto do protocolo TCP/IP que é responsável pelo endereçamento IP, roteamento, e fragmentação e montagem dos pacotes IP. |
| Itens para inicializar | Qualquer arquivo colocado nessa pasta será executado quando o computador iniciar. Por exemplo uma tela de boas-vindas, um arquivo de som, um aviso de calendário ou uma aplicação pode ser um item para inicializar. |
| Java applet | Um programa em Java que é projetado para ser executado somente em uma página web. Para usar um aplicativo em uma página web, você deve especificar o nome do aplicativo e o tamanho (comprimento e largura em pixels) que o aplicativo pode utilizar. Quando a página da web é acessada, o navegador descarrega-a de um servidor e executa na máquina do usuário (o cliente). Os aplicativos diferem dos programas em que eles são comandados por um protocolo estrito de segurança.<br><br>Por exemplo, mesmo um aplicativo funcione em um cliente, eles não podem ler ou escrever dados na máquina do cliente. Adicionalmente, os aplicativos são mais restringidos de modo que só podem ler e escrever dados nos domínios aos quais servem. |
| Linha de comando | Na interface de linha de comando, os usuários digitam os comando em um espaço fornecido diretamente na tela usando comandos da linguagem. |
| Memória | São áreas internas de armazenamento do computador. O termo memória identifica o armazenamento de dados que vem em forma de chips. Todo computador vem com |

| | |
|---|---|
| | uma certa quantidade de memória física, geralmente referida com memória RAM. |
| Navegador | Termo simplificado para navegador da web, um programa utilizado para localizar e exibir páginas da Internet. Os dois mais populares são Netscape Navigator e Microsoft Internet Explorer. Ambos são navegadores gráficos o que significa que podem exibir tanto gráficos como texto. Em adição, os navegadores mais modernos podem apresentar informações multimídia, como som e vídeo, através de plugins para alguns formatos. |
| Não heurística | Esse método de verificação confia em definições de vírus específicas. A vantagem da verificação não heurística é que ela não pode ser enganada por algo pode parecer um vírus, e não gera falsos alarmes. |
| Phishing | O ato de enviar e-mail a um usuário declarando falsamente ser uma empresa legítima em uma tentativa de enganar o usuário a entregar informações que serão usadas para roubo de identidade. O e-mail direciona o usuário a uma página web onde é perguntado a fornecer informação pessoal, tais como senhas, cartão de crédito, cadastros e contas em bancos, que a empresa legítima em questão já possui. A página web, no entanto, é falsa e existe apenas para roubar informação do usuário. |
| Porta | Uma interface no computador na qual você pode conectar um dispositivo. Computadores pessoais possuem vários tipos de portas. Internamente, existem vários tipos de portas conectando unidades de disco, monitores e teclados. Externamente, os computadores pessoais possuem portas conectando modems, impressoras, mouse e outros dispositivos periféricos.<br><br>Em redes TCP/IP e UDP, um ponto final a uma conexão lógica. A número da porta identifica que tipo de porta é. Por exemplo, porta 80 é usada para tráfego HTTP. |
| Programas compactados | Um arquivo em formato compactado. Muitos sistemas operacionais e programas contêm comando que permitem a você compactar um arquivo de modo que ocupe menos memória. Por exemplo: suponha que você tenha um texto que contém dez caracteres de espaço |

| | |
|---|---|
| | consecutivos. Normalmente, isso requereria dez bytes de armazenamento.<br><br>Entretanto, um programa que compacta arquivos substituiria os caracteres de espaço por caractere especial série-espaço seguido do número de espaços que estão sendo substituídos. Esta é apenas uma técnica de compactação, existem muitas outras. |
| Script | Outro termo para um arquivo de macro ou arquivo de comandos, um script é uma lista de comandos que podem ser executados sem a interação do usuário. |
| Setor de boot | O setor de boot é um setor no começo de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster, e assim por diante). Para inicializar os discos, o setor de boot também um programa que carrega o sistema operacional. |
| Spam | Lixo eletrônico em forma de mensagens. Normalmente conhecido como e-mail não solicitado. |
| Spyware | Qualquer software que coleta informação do usuário através da conexão de Internet sem o seu consentimento, normalmente para propósitos de propaganda. Aplicativos spyware são tipicamente distribuídos de forma oculta juntamente com programas freeware ou shareware que podem ser baixados da Internet; no entanto, deve ser notado que a maioria dos programas shareware e freeware não apresentam spyware. Uma vez instalado, o spyware monitora a atividade do usuário na Internet e transmite essa informação de forma oculta para outra pessoa. O spyware pode coletar também endereços de e-mail e até mesmo número de cartões de crédito e senhas.<br><br>A similaridade do spyware com o cavalo de tróia é que o usuário instala algo que não deseja instalando algum outro produto. Um modo comum de se tornar uma vítima de spyware é baixar alguns programas de compartilhamento de arquivos (peer-to-peer) que estão disponíveis hoje em dia. |

| | |
|---|---|
| | Colocando de lado as questões de ética e privacidade, o spyware prejudica o usuário consumindo memória do computador e conexão com a Internet quando manda a informação de volta a sua base usando a conexão de Internet do usuário. Porque o spyware usa a memória e os recursos do sistema, os aplicativos sendo executados podem levar o sistema ao colapso ou instabilidade geral. |
| TCP/IP | Transmission Control Protocol/Internet Protocol - Protocolo de controle de transmissão / protocolo da Internet. Um conjunto de protocolos largamente utilizados na Internet que fornece comunicação através de redes de computadores interconectadas com diversas arquiteturas de hardware e vários sistemas. O TCP/IP inclui padrões de como os computadores comunicam e convenções para conexões da rede e roteamento de tráfego. |
| Trojan | Um programa destrutivo que oculta uma aplicação benigna. Ao contrário do vírus, um cavalo de tróia não se replica mas pode ser muito destrutivo. Uma dos tipos mais incidentes de cavalos de tróia é um programa que diz se livras dos vírus do seu computador, mas ao invés disso ele introduz vírus em seu computador.<br><br>O termo vem da estória de Ilíada de Homero, na qual os gregos deram um cavalo de madeira gigante seus inimigos, os Troianos como uma oferta de paz. Mas depois dos troianos arrastarem o cavalo para dentro dos muros da cidade, os soldados Gregos saíram furtivamente da barriga do cavalo e abriram os portões da cidade, permitindo que seus compatriotas derrubassem e capturassem Tróia. |
| Unidade de disco | É uma máquina que lê e escreve dados em um disco.<br><br>Uma unidade de disco rígido lê e escreve em um disco rígido.<br><br>Uma unidade de disquete acessa disquetes.<br><br>Os discos rígidos podem ser internos (armazenado dentro do computador) ou externos (armazenado em uma caixa separada que está conectada ao computador). |

| | |
|---|---|
| Vírus | Um programa ou uma parte do código que é carregado no seu computador sem o seu conhecimento e se executa contra a sua vontade. A maioria dos vírus pode também se duplicar. Todos os computadores são feitos pelo homem. Um simples vírus pode fazer uma cópia dele mesmo repetidamente é fácil de se produzir. Mesmo um simples vírus é perigoso porque pode rapidamente usar toda memória disponível a fazer os sistema parar. O tipo de vírus mais perigoso é aquele que é capaz de transmitir-se através de uma rede ou contornando sistemas de segurança. |
| Vírus de boot | Um vírus que infecta o setor de boot do disco rígido ou de um disquete. Uma tentativa de inicialização com um disquete infectado com vírus de boot fará com que o vírus se torne ativo na memória. Toda vez que você reiniciar seu sistema daquele ponto em diante, você terá um vírus ativo na memória. |
| Vírus de macro | Um tipo de vírus de computador que é codificado como uma macro dentro de um documento. Muitas aplicações, como Microsoft Word e Excel, suportam poderosa linguagem de macro.<br><br>Essas aplicações permitem a você colocar uma macro em um documento, e mandam a macro ser executada cada vez que o documento é aberto. |
| Vírus polimórfico | Um vírus que muda sua forma cada vez que um arquivo é infectado. Como não têm nenhum padrão binário consistente, tais vírus são duros de identificar. |
| Worm | Um programa que se propaga pela rede, se reproduzindo enquanto isso. Ele não pode se anexar a outros programas. |